Cisco IOS IPv6 Command Reference

July 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 IPv6 Command Reference

Introduction

This book describes the commands used to configure and monitor IPv6. The commands in this book are organized alphabetically.

For IPv6 configuration information and examples, refer to the *Cisco IOS IPv6 Configuration Guide*.

Cisco IOS IPv6 Command Reference

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*}

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. This keyword might return user profile information such as what is generated by the **autocommand** command.
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 the 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 failures.
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 message, by a remote AAA server.

Defaults

AAA accounting is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.3	This command was introduced.
12.0(5)T	Group server support was added.
12.1(1)T	The **broadcast** keyword was added on the Cisco AS5300 and Cisco AS5800 universal access servers.
12.1(5)T	The **auth-proxy** keyword was added.
12.2(1)DX	The **vrf** keyword and *vrf-name* argument were added 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.
12.2(15)B	The tunnel and tunnel-link accounting methods were introduced.
12.3(4)T	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.

Table 1 contains descriptions of keywords for AAA accounting methods.

Table 1 aaa accounting Methods

Keyword	Description
group *group-name*	Uses a subset of RADIUS or TACACS+ servers for accounting as defined by the server group *group-name* argument.
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.

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 VRF is 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 This 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 start-stop radius** 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 enable IEEE 802.1x accounting:

```
aaa accounting dot1x default start-stop group radius
aaa accounting system default start-stop group radius
```

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.
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 multicast default

To enable authentication, authorization, and accounting (AAA) accounting of IPv6 multicast services for billing or security purposes when you use RADIUS, use the **aaa accounting multicast default** command in global configuration mode. To disable AAA accounting for IPv6 multicast services, use the **no** form of this command.

aaa accounting multicast default [**start-stop** | **stop-only**] [**broadcast**] [*method1*] [*method2*] [*method3*] [*method4*]

no aaa accounting multicast default [**start-stop** | **stop-only**] [**broadcast**] [*method1*] [*method2*] [*method3*] [*method4*]

Syntax Description

start-stop	(Optional) 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	(Optional) Sends a "stop" accounting notice at the end of the requested user process.
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.
method1, *method2*, *method3*, *method4*	(Optional) Method lists that specify an accounting method or multiple accounting methods to be used for accounting.

Command Default

AAA accounting for multicast is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

Note Including information about IPv6 addresses in accounting and authorization records transmitted between the router and the RADIUS or TACACS+ server is supported. However, there is no support for using IPv6 to communicate with that server. The server must have an IPv4 address.

Use the **aaa accounting multicast default** command to enable AAA accounting for multicast. 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.

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. When using the **aaa accounting multicast default** command, you have the option of choosing one or all four existing named access lists, each of which specifies a RADIUS host or server group.

If the **aaa accounting multicast default** 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.

For minimal accounting, include the **stop-only** keyword to send a "stop" record accounting notice at the end of the requested user process. For more accounting, you can include the **start-stop** keyword, so that RADIUS 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.

When AAA accounting is activated, the network access server monitors RADIUS accounting attributes pertinent to the connection. 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, refer to the appendix "RADIUS Attributes" in the *Cisco IOS Security Configuration Guide*.

Examples

The following example enables AAA accounting of IPv6 multicast services for billing or security purposes when RADIUS is used:

```
Router(config)# aaa accounting multicast default
```

Related Commands

Command	Description
aaa authorization multicast default	Sets parameters that restrict user access to an IPv6 network.

aaa accounting send counters ipv6

To send IPv6 counters in the stop record to the accounting server, use the **aaa accounting send counters ipv6** command in global configuration mode. To stop sending IPv6 counters, use the **no** form of this command.

aaa accounting send counters ipv6

no aaa accounting send counters ipv6

Syntax Description

This command has no arguments or keywords.

Defaults

IPv6 counters in the stop records are not sent to the accounting server.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.

Usage Guidelines

The **aaa accounting send counters ipv6** command sends IPv6 counters in the stop record to the accounting server.

Examples

The following example shows how enable the router to send IPv6 counters in the stop record to the accounting server:

```
Router(config)# aaa accounting send counters ipv6
```

aaa accounting send stop-record always

To send a stop record whether or not a start record was sent, use the **aaa accounting send stop-record always** command in global configuration mode. To disable sending a stop record, 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

A stop record is not sent.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines

When the **aaa accounting send stop-record always** command is enabled, accounting stop records are sent, even if their corresponding accounting starts were not sent out previously. This command enables stop records to be sent whether local authentication, or other authentication, is configured.

When a session is terminated on a Network Control Protocol (NCP) timeout, a stop record needs to be sent, even if a start record was not sent.

Examples

The following example shows how to enable stop records to be sent always when an NCP timeout occurs, whether or not a start record was sent:

```
Router(config)# aaa accounting send stop-record always
```

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 2.

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 2.

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 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 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 shows how to create a 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 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 3.

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 3, 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 3 describes the method keywords.

Table 3 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 configuration default

To download static route configuration information from the authorization, authentication, and accounting (AAA) server using TACACS+ or RADIUS, use the **aaa authorization configuration default** command in global configuration mode. To remove static route configuration information, use the **no** form of this command.

aaa authorization configuration default {**radius** | **tacacs+**}

no aaa authorization configuration default

Syntax Description

radius	RADIUS static route download.
tacacs+	TACACS+ static route download.

Defaults

No configuration authorization is defined.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2(13)T	Support for IPv6 was added.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Examples

The following example downloads static route information using a TACACS+ server:

```
aaa authorization configuration default tacacs+
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
aaa route download	Enables the download static route feature and sets the amount of time between downloads.
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 authorization multicast default

To enable authentication, authorization, and accounting (AAA) authorization and set parameters that restrict user access to an IPv6 multicast network, use the **aaa authorization multicast default** command in global configuration mode. To disable authorization for a function, use the **no** form of this command.

aaa authorization multicast default [*method*]

no aaa authorization multicast default [*method*]

Syntax Description

method3, *method4*	(Optional) Specifies one or two authorization methods that can be used for authorization. A method may be any one of the keywords listed in Table 3.

Command Default

Authorization is disabled for all actions.

Command Modes

Global configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

Note Including information about IPv6 addresses in accounting and authorization records transmitted between the router and the RADIUS or TACACS+ server is supported. However, there is no support for using IPv6 to communicate with that server. The server must have an IPv4 address.

Use the **aaa authorization multicast default** command to enable authorization. Method lists for authorization define the ways authorization will be performed and the sequence in which these methods will be performed. A method list is a named list describing the authorization methods to 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 IPv6 software uses the first method listed to authorize users for specific network services; if that method fails to respond, the Cisco IOS IPv6 software selects the next method listed in the method list. This process continues until there is successful communication with a listed authorization method, or all methods defined are exhausted.

Note The Cisco IOS IPv6 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 local username database responds by denying the user services—the authorization process stops, and no other authorization methods are attempted.

If the **aaa authorization multicast default** command for a particular authorization type is issued without a named method list specified, the default method list is automatically applied to all lines or interfaces (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.

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

Method keywords are described in Table 3.

Table 4 aaa authorization Methods

Keyword	Description
group radius	Uses the list of all RADIUS servers for authentication as defined by the **aaa group server radius** command.
group *group-name*	Uses a subset of RADIUS servers for accounting as defined by the **server group** *group-name* command.
if-authenticated	Allows the user to access the requested function if the user is authenticated.
local	Uses the local database for authorization.
none	No authorization is performed.

Cisco IOS IPv6 software supports the following methods for authorization:

- 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.
- If-Authenticated—The user is allowed to access the requested function provided the user has been authenticated successfully.
- None—The network access server does not request authorization information; authorization is not performed over this line or interface.
- 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 via the local database.

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

- Network—Applies to network connections. This can include a PPP, Serial Line Internet Protocol (SLIP), or AppleTalk Remote Access (ARA) connection.
- EXEC—Applies to the attributes associated with a user EXEC terminal session.
- Commands—Applies to the EXEC mode commands and user issues. Command authorization attempts authorization for all EXEC mode commands, including global configuration commands, associated with a specific privilege level.
- Reverse Access—Applies to reverse Telnet sessions.
- Configuration—Applies to the configuration downloaded from the AAA server.

The **authorization** command causes a request packet containing a series of AV pairs to be sent to the RADIUS 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 refuse authorization.

For a list of supported RADIUS attributes, refer to the appendix "RADIUS Attributes" in the *Cisco IOS Security Configuration Guide*.

Examples

The following example enables AAA authorization and sets default parameters that restrict user access to an IPv6 multicast network:

```
Router(config)# aaa authorization multicast default
```

Related Commands

Command	Description
aaa accounting multicast default	Enables AAA accounting of IPv6 multicast services for billing or security purposes when you use RADIUS.
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
radius-server host	Specifies a RADIUS server host.
username	Establishes a username-based authentication system.

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 5 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 5 lists words that cannot be used as the *group-name* argument.

Table 5 Words That Cannot Be Used As the group-name Argument

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

Table 5 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 5 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.
Cisco IOS XE Release 3.2S	This command was modified. Support for IPv6 was added.

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 5 lists the keywords that cannot be used for the *group-name* argument value.

Table 6 Words That Cannot Be Used As the group-name Argument

Word
auth-guest
enable

Table 6 Words That Cannot Be Used As the group-name Argument (continued)

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

Examples

The following example shows the configuration of an AAA server group 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 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.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

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.

accept-lifetime

To set the time period during which the authentication key on a key chain is received as valid, use the **accept-lifetime** command in key chain key configuration mode. To revert to the default value, use the **no** form of this command.

accept-lifetime *start-time* {**infinite** | *end-time* | **duration** *seconds*}

no accept-lifetime [*start-time* {**infinite** | *end-time* | **duration** *seconds*}]

Syntax Description

start-time	Beginning time that the key specified by the **key** command is valid to be received. The syntax can be either of the following: *hh*:*mm*:*ss Month date year* *hh*:*mm*:*ss date Month year* • *hh*—hours • *mm*—minutes • *ss*—seconds • *Month*—first three letters of the month • *date*—date (1–31) • *year*—year (four digits) The default start time and the earliest acceptable date is January 1, 1993.
infinite	Key is valid to be received from the *start-time* value on.
end-time	Key is valid to be received from the *start-time* value until the *end-time* value. The syntax is the same as that for the *start-time* value. The *end-time* value must be after the *start-time* value. The default end time is an infinite time period.
duration *seconds*	Length of time (in seconds) that the key is valid to be received. The range is from 1 to 2147483646.

Command Default

The authentication key on a key chain is received as valid forever (the starting time is January 1, 1993, and the ending time is infinite).

Command Modes

Key chain key configuration (config-keychain-key)

Command History

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

Only DRP Agent, Enhanced Interior Gateway Routing Protocol (EIGRP), and Routing Information Protocol (RIP) Version 2 use key chains.

Specify a *start-time* value and one of the following values: **infinite**, *end-time*, or **duration** *seconds.*

We recommend running Network Time Protocol (NTP) or some other time synchronization method if you assign a lifetime to a key.

If the last key expires, authentication will continue and an error message will be generated. To disable authentication, you must manually delete the last valid key.

Examples

The following example configures a key chain named chain1. The key named key1 will be accepted from 1:30 p.m. to 3:30 p.m. and will be sent from 2:00 p.m. to 3:00 p.m. The key named key2 will be accepted from 2:30 p.m. to 4:30 p.m. and will be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or a discrepancy in the set time of the router. There is a 30-minute leeway on each side to handle time differences.

```
Router(config)# interface ethernet 0
Router(config-if)# ip rip authentication key-chain chain1
Router(config-if)# ip rip authentication mode md5
!
Router(config)# router rip
Router(config-router)# network 172.19.0.0
Router(config-router)# version 2
!
Router(config)# key chain chain1
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string key1
Router(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 14:00:00 Jan 25 1996 duration 3600
Router(config-keychain-key)# exit
Router(config-keychain)# key 2
Router(config-keychain)# key-string key2
Router(config-keychain)# accept-lifetime 14:30:00 Jan 25 1996 duration 7200
Router(config-keychain)# send-lifetime 15:00:00 Jan 25 1996 duration 3600
```

The following example configures a key chain named chain1 for EIGRP address-family. The key named key1 will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. The key named key2 will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or a discrepancy in the set time of the router. There is a 30-minute leeway on each side to handle time differences.

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# network 10.0.0.0
Router(config-router-af)# af-interface ethernet0/0
Router(config-router-af-interface)# authentication key-chain trees
Router(config-router-af-interface)# authentication mode md5
Router(config-router-af-interface)# exit
Router(config-router-af)# exit
Router(config-router)# exit
Router(config)# key chain chain1
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string key1
Router(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 14:00:00 Jan 25 1996 duration 3600
Router(config-keychain-key)# exit
Router(config-keychain)# key 2
```

```
Router(config-keychain-key)# key-string key2
Router(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 15:00:00 Jan 25 1996 duration 3600
```

Related Commands

Command	Description
key	Identifies an authentication key on a key chain.
key chain	Defines an authentication key-chain needed to enable authentication for routing protocols.
key-string (authentication)	Specifies the authentication string for a key.
send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.
show key chain	Displays authentication key information.

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 merge mode.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
12.2(33)SXI4	Support for IPv6 was added. The **prefer vlan** keyword combination is not supported in 12.2(33)SXI4.
12.2(54)SG	This command was modified. Support for Cisco IOS Release 12.2(54)SG was added.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY. The **prefer vlan** keyword combination is not supported for IPv6.

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).

In Cisco IOS Release 12.2(33)SXI4, prefer port and merge modes are supported on the Layer 2 interface. A Layer 2 interface can have one IPv6 ACL applied in the ingress, or inbound, direction only.

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.

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 (Mobile IPv6)

To specify the home address of the IPv6 mobile node, use the **address** command in home-agent configuration mode or IPv6 mobile router host configuration mode. To remove a host configuration, use the **no** form of this command.

address {*ipv6-address* | **autoconfig**}

no address

Syntax Description

ipv6-address	Specifies a home address for the mobile node. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
autoconfig	Allows any IPv6 address to be used.

Command Default

No home address is specified for the mobile router.

Command Modes

Home-agent configuration (config-ha)
IPv6 mobile router host configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.
12.4(20)T	IPv6 network mobility (NEMO) functionality was added.

Usage Guidelines

The **address** command in IPv6 home-agent configuration mode specifies the home address of the mobile node. The *ipv6-address* argument can be used to configure a specific IPv6 address, or the **autoconfig** keyword can be used to allow any IPv6 address as the home address of the IPv6 mobile node.

Do not configure two separate groups with the same IPv6 address. For example, host group group1 and host group group2 cannot both have the same home address of baba::1.

When the **address** command is configured with a specific IPv6 address, the **nai** command, which configures the network address identifier (NAI), cannot be configured using the *@realm* argument. For example, the following **nai** command configuration would not be valid because the **address** command is configured with the specific address baba::1:

```
host group engineering
  nai  @cisco.com
  address baba::1
```

Examples

In the following example, the user enters home agent configuration mode, creates a host group named group1, and configures any IPv6 address to be used for the mobile node:

```
Router(config)# ipv6 mobile home-agent
Router(config-ha)# host group group1
```

```
Router(config-ha)# address autoconfig
```

Related Commands

Command	Description
host group	Creates a host configuration in IPv6 Mobile.
ipv6 mobile home-agent (global configuration)	Enters home agent configuration mode.
nai	Specifies the NAI for the IPv6 mobile node.

address ipv6 (TACACS+)

To configure the IPv6 address of the TACACS+ server, use the **address ipv6** command in TACACS+ server configuration mode. To remove the IPv6 address, use the **no** form of this command.

address ipv6 *ipv6-address*

no address ipv6 *ipv6-address*

Syntax Description

ipv6-address	The private TACACS+ server host.

Command Default

No TACACS+ server is configured.

Command Modes

TACACS+ server configuration (config-server-tacacs)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines

Use the **address ipv6** (**TACACS+**) command after you have enabled the TACACS+ server using the **tacacs server** command.

Examples

The following example shows how to specify the IPv6 address on a TACACS+ server named server1:

```
Router (config)# tacacs server server1
Router(config-server-tacacs)# address ipv6 2001:0DB8:3333:4::5
```

Related Commands

Command	Description
tacacs server	Configures the TACACS+ server for IPv6 or IPv4 and enters config server tacacs mode.

address-family (EIGRP)

To enter address-family configuration mode to configure an Enhanced Interior Gateway Routing Protocol (EIGRP) routing instance, use the **address-family** (EIGRP) command in router configuration mode. To remove the address-family from the EIGRP configuration, use the **no** form of this command.

EIGRP Autonomous-System Configuration

address-family ipv4 [**unicast**] **vrf** *vrf-name* [**autonomous-system** *autonomous-system-number*]

no address-family ipv4 [**unicast**] **vrf** *vrf-name* [**autonomous-system** *autonomous-system-number*]

EIGRP Named IPv4 Configuration

address-family ipv4 [**multicast**] [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*

no address-family ipv4 [**multicast**] [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*

EIGRP Named IPv6 Configuration

address-family ipv6 [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*

no address-family ipv6 [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*

Syntax Description

ipv4	Selects the IPV4 protocol address-family.
ipv6	Selects the IPV6 protocol address-family. IPv6 is supported only in EIGRP named configurations.
multicast	(Optional) Specifies the multicast address-family. This keyword is available only in EIGRP named IPv4 configurations.
unicast	(Optional) Specifies the unicast address-family.
autonomous-system *autonomous-system- number*	(Optional) Specifies the autonomous system number. This keyword/argument pair is required for EIGRP named configurations.
vrf *vrf-name*	(Optional) Specifies the name of the VRF. This keyword/argument pair is required for EIGRP AS configurations.

Command Default

No EIGRP process is running.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.

Release	Modification
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.
15.0(1)M	This command was modified. The **autonomous-system** keyword is required for named configurations.
12.2(33)SRE	This command was modified. The **autonomous-system** keyword is required for named configurations.
12.2(33)XNE	This command was modified. The **autonomous-system** keyword is required for named configurations.
Cisco IOS XE Release 2.5	This command was modified. The **autonomous-system** keyword is required for named configurations.
12.2(33)SXI4	This command was modified. The **autonomous-system** keyword is required for named configurations.

Usage Guidelines

The **address-family** (EIGRP) command is used to configure IPv4 or IPv6 address-family sessions under EIGRP. To leave address-family configuration mode without removing the address family configuration, use the **exit-address-family** command.

EIGRP Autonomous-System Configuration

Use the **router eigrp** *number* command to configure an EIGRP autonomous-system (AS) configuration.

In this configuration, EIGRP VPNs can be configured only under IPv4 address-family configuration mode. A virtual routing and forwarding instance (VRF) and route distinguisher must be defined before the address family session can be created.

It is recommended that you configure an autonomous-system number when the address-family is configured, either by entering the **address-family** command or the **autonomous-system** command.

EIGRP Named Configuration

Use the **router eigrp** *virtual-name* command to configure an EIGRP named configuration.

In this configuration, EIGRP VPNs can be configured in IPv4 and IPv6 named configurations. A virtual routing and forwarding instance (VRF) and a route distinguisher may or may not be used to create the address-family.

If a VRF is not used in creating the address-family, the EIGRP VPN instance assumes the default route distinguisher and will communicate with the default route distinguisher of other routers in the same network.

EIGRP VPNs can be configured under EIGRP named configurations. A virtual routing and forwarding instance (VRF) and route distinguisher must be defined before the address-family session can be created.

A single EIGRP routing process can support multiple VRFs. The number of VRFs that can be configured is limited only by available system resources on the router, which is determined by the number of VRFs, running processes, and available memory. However, only a single VRF can be supported by each VPN, and redistribution between different VRFs is not supported.

MPLS VPN support between PE and CE routers is configured only on PE routers that provide VPN services over the service provider backbone. The customer site does not require any changes to equipment or configurations to support the EIGRP VPN. A metric must be configured for routes to be advertised to the CE router. The metric can be configured using the **redistribute (IP)** command or configured with the **default-metric** (EIGRP) command.

Examples

The following example configures an IPv4 address-family session for the VRF named RED in Cisco IOS releases prior to Cisco IOS Release 15.0(1)M, 12.2(33)SRE, 12.2(33)XNE and Cisco IOS XE Release 2.5:

```
Router(config)# ip vrf RED
Router(config-vrf)# rd 1:1
Router(config-vrf)# exit
Router(config)# router eigrp 1
Router(config-router)# address-family ipv4 vrf RED
Router(config-router-af)# autonomous-system 101
Router(config-router-af)# network 172.16.0.0
Router(config-router-af)# default-metric 10000 100 255 1 1500
Router(config-router-af)# exit-address-family
```

The following examples configure a single VRF named VRF-RED in Cisco IOS Release 15.0(1)M, 12.2(33)SRE, 12.2(33)XNE and Cisco IOS XE Release 2.5 and later releases:

```
Router(config)# ip vrf VRF-RED
Router(config-vrf)# rd 1:1
Router(config-vrf)# exit
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 vrf VRF-RED autonomous-system 1
Router(config-router-af)# network 10.0.0.0 0.0.0.255
Router(config-router-af)# topology base
Router(config-router-topology)# default-metric 10000 100 255 1 1500
Router(config-router-topology)# exit-af-topology
Router(config-router-af)# exit-address-family
```

The following example configures a non-VRF address-family in Cisco IOS Release 15.0(1)M, 12.2(33)SRE, 12.2(33)XNE and Cisco IOS XE Release 2.5, and later releases:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 3
Router(config-router-af)# network 10.0.0.0 0.0.0.255
Router(config-router-af)# topology base
Router(config-router-af-topology)# default-metric 10000 100 255 1 1500
Router(config-router-af- topology)# exit-af-topology
Router(config-router-af)# exit-address-family
```

Related Commands

Command	Description
autonomous-system (EIGRP)	Configures the autonomous-system number for an EIGRP routing process to run within a VRF instance.
default-metric (EIGRP)	Sets metrics for EIGRP.
exit-address-family	Exits address-family configuration mode.
network (EIGRP)	Specifies a list of networks for the EIGRP routing process.
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.

address-family ipv4 (BGP)

To enter address family or router scope address family configuration mode to configure a routing session using standard IP Version 4 (IPv4) address prefixes, use the **address-family ipv4** command in router configuration or router scope configuration mode. To exit address family configuration mode and remove the IPv4 address family configuration from the running configuration, use the **no** form of this command.

Syntax Available Under Router Configuration Mode

address-family ipv4 [**mdt** | **multicast** | **tunnel** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*]

no address-family ipv4 [**mdt** | **multicast** | **tunnel** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*]

Syntax Available Under Router Scope Configuration Mode

address-family ipv4 [**mdt** | **multicast** | **unicast**]

no address-family ipv4 [**mdt** | **multicast** | **unicast**]

Syntax Description

mdt	(Optional) Specifies an IPv4 multicast distribution tree (MDT) address family session.
multicast	(Optional) Specifies IPv4 multicast address prefixes.
tunnel	(Optional) Specifies an IPv4 routing session for multipoint tunneling.
unicast	(Optional) Specifies IPv4 unicast address prefixes. This is the default.
vrf *vrf-name*	(Optional) Specifies the name of the VPN routing and forwarding (VRF) instance to associate with subsequent IPv4 address family configuration mode commands.

Command Default

IPv4 address prefixes are not enabled.

Command Modes

Router configuration (config-router)
Router scope configuration (config-router-scope)

Command History

Release	Modification
12.0(5)T	This command was introduced. This command replaced the **match nlri** and **set nlri** commands.
12.0(28)S	This command was integrated into Cisco IOS Release 12.0(28)S, and the **tunnel** keyword was added.
12.0(29)S	The **mdt** keyword was added.
12.0(30)S	Support for the Cisco 12000 series Internet router was added.
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)SRB	Support for the router scope configuration mode was added.

Release	Modification
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
12.4(20)T	The **mdt** keyword was added.

Usage Guidelines

The **address-family ipv4** command replaces the **match nlri** and **set nlri** commands. The **address-family ipv4** command places the router in address family configuration mode (prompt: `config-router-af)`, from which you can configure routing sessions that use standard IPv4 address prefixes. To leave address family configuration mode and return to router configuration mode, type **exit**.

Note Routing information for address family IPv4 is advertised by default for each BGP routing session configured with the **neighbor remote-as** command unless you enter the **no bgp default ipv4-unicast** command before configuring the **neighbor remote-as** command.

The **tunnel** keyword is used to enable the tunnel subaddress family identifier (SAFI) under the IPv4 address family identifier. This SAFI is used to advertise the tunnel endpoints and the SAFI-specific attributes (which contain the tunnel type and tunnel capabilities). Redistribution of tunnel endpoints into the BGP IPv4 tunnel SAFI table occurs automatically when the tunnel address family is configured. However, peers need to be activated under the tunnel address family before the sessions can exchange tunnel information.

The **mdt** keyword is used to enable the MDT SAFI under the IPv4 address family identifier. This SAFI is used to advertise tunnel endpoints for inter-AS multicast VPN peering sessions.

If you specify a**ddress-family ipv4 multicast**, you will then specify the **network** *network-number* [**mask** *network-mask*] command. The **network** command advertises (injects) the specified network number and mask into the multicast BGP database. This route must exist in the forwarding table installed by an IGP (that is, by eigrp, ospf, rip, igrp, static, or is-is), but not bgp.

In Cisco IOS Release 12.2(33)SRB and later releases, the ability to use address family configuration under the router scope configuration mode was introduced. The scope hierarchy can be defined for BGP routing sessions and is required to support Multi-Topology Routing (MTR). To enter the router scope configuration mode, use the **scope** command, which can apply globally or for a specific VRF. When using the scope for a specific VRF, only the **unicast** keyword is available.

Examples

The following example places the router in address family configuration mode for the IPv4 address family:

```
Router(config)# router bgp 50000
Router(config-router)# address-family ipv4
Router(config-router-af)#
```

Multicast Example

The following example places the router in address family configuration mode and specifies only multicast address prefixes for the IPv4 address family:

```
Router(config)# router bgp 50000
Router(config-router)# address-family ipv4 multicast
Router(config-router-af)#
```

Unicast Example

The following example places the router in address family configuration mode and specifies unicast address prefixes for the IPv4 address family:

```
Router(config)# router bgp 50000
Router(config-router)# address-family ipv4 unicast
Router(config-router-af)#
```

VRF Example

The following example places the router in address family configuration mode and specifies **cisco** as the name of the VRF instance to associate with subsequent IPv4 address family configuration mode commands:

```
Router(config)# router bgp 50000
Router(config-router)# address-family ipv4 vrf cisco
Router(config-router-af)#
```

Note Use this form of the command, which specifies a VRF, only to configure routing exchanges between provider edge (PE) and customer edge (CE) devices.

Tunnel Example

The following example places the router in tunnel address family configuration mode:

```
Router(config)# router bgp 100
Router(config-router)# address-family ipv4 tunnel
Router(config-router-af)#
```

MDT Example

The following example shows how to configure a router to support an IPv4 MDT address-family session:

```
Router(config)# router bgp 45000
Router(config-router)# address-family ipv4 mdt
Router(config-router-af)#
```

Router Scope Configuration Mode Example

The following example shows how to configure the IPv4 address family under router scope configuration mode. In this example, the scope hierarchy is enabled globally. The router enters router scope address family configuration mode, and only multicast address prefixes for the IPv4 address family are specified:

```
Router(config)# router bgp 50000
Router(config-router)# scope global
Router(config-router-scope)# address-family ipv4 multicast
Router(config-router-scope-af)#
```

Related Commands

Command	Description
address-family ipv6	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard IPv6 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPN Version 4 address prefixes.
bgp default ipv4-unicast	Enables the IPv4 unicast address family on all neighbors.
neighbor activate	Enables the exchange of information with a BGP neighboring router.

Command	Description
neighbor remote-as	Adds an entry to the BGP or multiprotocol BGP neighbor table.
scope	Defines the scope for a BGP routing session and enters router scope configuration mode.

address-family ipv6

To enter address family configuration mode for configuring routing sessions such as Border Gateway Protocol (BGP) that use standard IPv6 address prefixes, use the **address-family ipv6** command in router configuration mode. To disable address family configuration mode, use the **no** form of this command.

address-family ipv6 [**vrf** *vrf-name*] [**unicast | multicast | vpnv6**]

no address-family ipv6 [**vrf** *vrf-name*] [**unicast | multicast | vpnv6**]

Syntax Description

vrf	(Optional) Specifies all Virtual Private Network (VPN) routing and forwarding (VRF) instance tables or a specific VRF table for IPv6 address.
vrf-name	(Optional) Names a specific VRF table for an IPv6 address.
unicast	(Optional) Specifies IPv6 unicast address prefixes.
multicast	(Optional) Specifies IPv6 multicast address prefixes.
vpnv6	(Optional) Specifies VPN Version 6 address prefixes.

Command Default

IPv6 address prefixes are not enabled. Unicast address prefixes are the default when IPv6 address prefixes are configured.

Note Routing information for address family IPv4 is advertised by default for each BGP routing session configured with the **neighbor remote-as** command unless you configure the **no bgp default ipv4-unicast** command before configuring the **neighbor remote-as** command.

Command Modes

Router configuration

Command History

Release	Modification
12.2(2)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 Release 12.2(14)S.
12.0(26)S	The **multicast** keyword was added to Cisco IOS Release 12.0(26)S.
12.3(4)T	The **multicast** keyword was added to Cisco IOS Release 12.3(4)T.
12.2(25)S	The **multicast** keyword was added to Cisco IOS Release 12.2(25)S.
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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	The **vrf** keyword and *vrf-name* argument were added to Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Release	Modification
Cisco IOS XE Release 2.1	The **vpnv6** keyword was added.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
12.2(33)SRE	This command was modified. It wasintegrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

The **address-family ipv6** command places the router in address family configuration mode (prompt: config-router-af), from which you can configure routing sessions that use standard IPv6 address prefixes.

Within address family configuration mode, use the question mark (?) online help function to display supported commands. The BGP commands supported in address family configuration mode configure the same functionality as the BGP commands supported in router configuration mode; however, the BGP commands in router configuration mode configure functionality only for the IPv4 unicast address prefix. To configure BGP commands and functionality for other address family prefixes (for example, the IPv4 multicast or IPv6 unicast address prefixes), you must enter address family configuration mode for those address prefixes using the **address-family ipv4** command or the **address-family ipv6** command.

Use the **multicast** keyword to specify an administrative distance for multicast BGP routes to be used in reverse path forwarding (RPF) lookups.

Examples

The following example places the router in address family configuration mode and specifies unicast address prefixes for the IPv6 address family:

```
Router(config)# router bgp 100
Router(config-router)# address-family ipv6 unicast
```

The following example places the router in address family configuration mode and specifies multicast address prefixes for the IPv6 address family:

```
Router(config)# router bgp 100
Router(config-router)# address-family ipv6 multicast
```

Related Commands

Command	Description
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard IPv4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard VPNv4 address prefixes.
address-family vpnv6	Enters address family configuration mode for configuring routing sessions, such as BGP, that use standard VPNv6 address prefixes
bgp default ipv4-unicast	Enables the IPv4 unicast address family on all neighbors.
neighbor activate	Enables the exchange of information with a BGP neighboring router.

address-family ipv6 (IS-IS)

To enter address family configuration mode for configuring Intermediate System-to-Intermediate System (IS-IS) routing sessions that use standard IPv6 address prefixes, use the **address-family ipv6** command in router configuration mode. To reset all IPv6-specific global configuration values to their default values, use the **no** form of this command.

address-family ipv6 [**unicast**]

no address-family ipv6 [**unicast**]

Syntax Description

unicast	(Optional) Specifies IPv6 unicast address prefixes.

Command Default

IPv6 address prefixes are not enabled. Unicast address prefixes are the default when IPv6 address prefixes are configured.

Command Modes

Router configuration

Command History

Release	Modification
12.2(8)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 Release 12.2(14)S.
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.
12.2(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 2.6	This command was introduced on Cisco ASR 1000 series routers.

Usage Guidelines

The **address-family ipv6** command places the router in address family configuration mode (prompt: config-router-af), from which you can configure IPv6-specific settings. To leave address family configuration mode and return to router configuration mode, enter the **exit-address-family** command.

Within address family configuration mode, use the question mark (?) online help function to display supported commands. Many of the IS-IS commands supported in address family configuration mode are identical in syntax to IS-IS commands supported in router configuration mode. Note that commands issued in address family configuration mode apply to IPv6 only, while the matching commands in router configuration mode are IPv4-specific.

Examples

The following example places the router in address family configuration mode for IS-IS and specifies unicast address prefixes for the IPv6 address family:

```
Router(config)# router isis area01
Router(config-router)# address-family ipv6 unicast
```

address-family ipv4 (OSPFv3)

To enter IPv4 address family configuration mode for Open Shortest Path First version 3 (OSPFv3), use the **address-family ipv4** command in OSPFv3 router configuration mode.

address-family ipv4 unicast

Syntax Description

unicast	Specifies IPv4 unicast address prefixes.

Command Default

Command Modes

OSPFv3 router configuration mode (config-router)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

Use the **address-family ipv4** command to configure the IPv4 address family in the OSPFv3 process. Only one address family can be configured per instance. Several IPv4 address family-specific commands are available once you have enabled the **address-family ipv4** command and entered IPv4 address family configuration mode.

Examples

The following example enters IPv4 address family configuration mode for OSPFv3:

```
Router(config-router)#address-family ipv4 unicast
Router(config-router-af)#
```

Related Commands

router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

address-family ipv6 (OSPFv3)

To enter IPv6 address family configuration mode for Open Shortest Path First version 3 (OSPFv3), use the **address-family ipv6** command in OSPFv3 router configuration mode.

address-family ipv6 unicast

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.

Command Default

Command Modes

OSPFv3 router configuration mode (config-router)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

Use the **address-family ipv6** command to configure the IPv6 address family in the OSPFv3 process. Only one address family can be configured per instance. Several IPv6 address family-specific commands are available once you have enabled the **address-family ipv6** command and entered IPv6 address family configuration mode.

Examples

The following example enters IPv6 address family configuration mode for OSPFv3:

```
Router(config-router)# address-family ipv6 unicast
Router(config-router-af)#
```

Related Commands

router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

address-family vpnv6

To place the router in address family configuration mode for configuring routing sessions, such as Border Gateway Protocol (BGP), that use standard VPNv6 address prefixes, use the **address-family vpnv6** command in router BGP configuration mode. To disable address family configuration mode, use the **no** form of this command.

address-family vpnv6 [**unicast**]

no address-family vpnv6 [**unicast**]

Syntax Description

unicast	(Optional) Specifies VPN Version 6 unicast address prefixes.

Command Default

VPN Version 6 address prefixes are not enabled. Unicast address prefixes are the default when VPN Version 6 address prefixes are configured.

Command Modes

Router BGP configuration

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 series routers.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

The **address-family vpnv6** command places the router in address family configuration mode, from which you can configure routing sessions that use VPN Version 6 address prefixes. An address family must be configured for each VPN routing/forwarding (VRF) on a provider edge (PE) router. Furthermore, a separate address family must be configured for carrying VPN-IPv6 routes between PE routers.

Examples

The following example places the router in address family configuration mode for the VPN Version 6 address family:

```
Router(config)# router bgp 100
Router(config-router)# address-family vpnv6
```

Related Commands

Command	Description
address-family ipv6	Enters address family configuration mode for configuring routing sessions such as BGP that use standard IPv6 address prefixes.
neighbor activate	Enables the exchange of information with a BGP neighbor.

address prefix

To specify an address prefix for address assignment, use the **address prefix** command in interface configuration mode. To remove the address prefix, use the **no** form of this command.

address prefix *ipv6-prefix* [**lifetime** {*valid-lifetime preferred-lifetime* | **infinite**}]

no address prefix

Syntax Description

ipv6-prefix	IPv6 address prefix.
lifetime {*valid-lifetime preferred-lifetime*	**infinite**}]	(Optional) Specifies a time interval (in seconds) that an IPv6 address prefix remains in the valid state. If the **infinite** keyword is specified, the time interval does not expire.

Command Default

No IPv6 address prefix is assigned.

Command Modes

DHCP pool configuration (config-dhcpv6)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

You can use the **address prefix** command to configure one or several address prefixes in an IPv6 DHCP pool configuration. Each time the IPv6 DHCP address pool is used, an address will be allocated from each of the address prefixes associated with the IPv6 DHCP pool.

Examples

The following example shows how to configure a pool called engineering with an IPv6 address prefix:

```
Router(config)# ipv6 dhcp pool engineering
Router(config-dhcpv6)# address prefix 2001:1000::0/64 lifetime infinite
```

Related Commands

Command	Description
ipv6 dhcp pool	Configures a DHCPv6 server configuration information pool and enters DHCPv6 pool configuration mode.

adjacency-check

To allow Intermediate System-to-Intermediate System (IS-IS) IPv6 or IPv4 protocol-support consistency checks performed on hello packets, use the **adjacency-check** command in address family configuration or router configuration mode. To disable consistency checks on hello packets, use the **no** form of this command.

adjacency-check

no adjacency-check

Syntax Description

This command has no arguments or keywords.

Command Default

The feature is enabled.

Command Modes

Address family configuration
Router configuration

Command History

Release	Modification
12.2(8)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 Release 12.2(14)S.
12.2(15)T	Support was added for router configuration mode.
12.2(18)S	Support was added for router configuration mode.
12.0(26)S	Support was added for router configuration mode.
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.
12.2(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

IS-IS performs consistency checks on hello packets and will form an adjacency only with a neighboring router that supports the same set of protocols. A router running IS-IS for both IPv4 and IPv6 will not form an adjacency with a router running IS-IS for IPv4 only.

Use the **no adjacency-check** command in address-family configuration mode to suppress the consistency checks for IPv6 IS-IS and allow an IPv4 IS-IS router to form an adjacency with a router running IPv4 IS-IS and IPv6. IS-IS will never form an adjacency between a router running IPv4 IS-IS only and a router running IPv6 only.

Use the **no adjacency-check** command in router configuration mode to suppress the IPv4 subnet consistency check and allow IS-IS to form an adjacency with other routers regardless of whether or not they have an IPv4 subnet in common. By default, IS-IS makes checks in hello packets for IPv4 address subnet matching with a neighbor. In multitopology mode, the IPv4 subnet consistency check is automatically suppressed.

Tip Use the **debug isis adjacency packets** command in privileged EXEC mode to check for adjacency errors. Error messages in the output may indicate where routers are failing to establish adjacencies.

Examples

In the following example, the network administrator wants to introduce IPv6 into an existing IPv4 IS-IS network. To ensure that the checking of hello packet checks from adjacent neighbors is disabled until all the neighbor routers are configured to use IPv6, the network administrator enters the **no adjacency-check** command.

```
Router(config)# router isis
Router(config-router)# address-family ipv6
Router(config-router-af)# no adjacency-check
```

In IPv4, the following example shows that the network administrator wants to introduce IPv6 into an existing IPv4 IS-IS network. To ensure that the checking of hello packet checks from adjacent neighbors is disabled until all the neighbor routers are configured to use IPv6, the network administrator enters the **no adjacency-check** command.

```
Router(config)# router isis
Router(config-router-af)# no adjacency-check
```

aggregate-address

To create an aggregate entry in a Border Gateway Protocol (BGP) database, use the **aggregate-address** command in address family or router configuration mode. To disable this function, use the **no** form of this command.

aggregate-address *address mask* [**as-set**] [**as-confed-set**] [**summary-only**] [**suppress-map** *map-name*] [**advertise-map** *map-name*] [**attribute-map** *map-name*]

no aggregate-address *address mask* [**as-set**] [**as-confed-set**] [**summary-only**] [**suppress-map** *map-name*] [**advertise-map** *map-name*] [**attribute-map** *map-name*]

Syntax Description

address	Aggregate address.
mask	Aggregate mask.
as-set	(Optional) Generates autonomous system set path information.
as-confed-set	(Optional) Generates autonomous confederation set path information.
summary-only	(Optional) Filters all more-specific routes from updates.
suppress-map *map-name*	(Optional) Specifies the name of the route map used to select the routes to be suppressed.
advertise-map *map-name*	(Optional) Specifies the name of the route map used to select the routes to create AS_SET origin communities.
attribute-map *map-name*	(Optional) Specifies the name of the route map used to set the attribute of the aggregate route.

Command Default

The atomic aggregate attribute is set automatically when an aggregate route is created with this command unless the **as-set** keyword is specified.

Command Modes

Address family configuration (config-router-af)
Router configuration (config-router)

Command History

Release	Modification
10.0	This command was introduced.
11.1(20)CC	The **nlri unicast**, **nlri multicast**, and **nlri unicast multicast** keywords were added.
12.0(2)S	The **nlri unicast**, **nlri multicast**, and **nlri unicast multicast** keywords were added.
12.0(7)T	The **nlri unicast**, **nlri multicast**, and **nlri unicast multicast** keywords were removed. Address family configuration mode support was added.
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.

Release	Modification
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(33)SRE	The **as-confed-set** keyword was added.
Cisco IOS XE Release 3.1S	This command was introduced on Cisco ASR 1000 series routers.

Usage Guidelines

You can implement aggregate routing in BGP and Multiprotocol BGP (mBGP) either by redistributing an aggregate route into BGP or mBGP, or by using the conditional aggregate routing feature.

Using the **aggregate-address** command with no keywords will create an aggregate entry in the BGP or mBGP routing table if any more-specific BGP or mBGP routes are available that fall within the specified range. (A longer prefix that matches the aggregate must exist in the Routing Information Base (RIB).) The aggregate route will be advertised as coming from your autonomous system and will have the atomic aggregate attribute set to show that information might be missing. (By default, the atomic aggregate attribute is set unless you specify the **as-set** keyword.)

Using the **as-set** keyword creates an aggregate entry using the same rules that the command follows without this keyword, but the path advertised for this route will be an AS_SET consisting of all elements contained in all paths that are being summarized. Do not use this form of the **aggregate-address** command when aggregating many paths, because this route must be continually withdrawn and updated as autonomous system path reachability information for the summarized routes changes.

Using the **as-confed-set** keyword creates an aggregate entry using the same rules that the command follows without this keyword. This keyword performs the same function as the **as-set** keyword, except that it generates autonomous confed set path information.

Using the **summary-only** keyword not only creates the aggregate route (for example, 192.*.*.*) but also suppresses advertisements of more-specific routes to all neighbors. If you want to suppress only advertisements to certain neighbors, you may use the **neighbor distribute-list** command, with caution. If a more-specific route leaks out, all BGP or mBGP routers will prefer that route over the less-specific aggregate you are generating (using longest-match routing).

Using the **suppress-map** keyword creates the aggregate route but suppresses advertisement of specified routes. You can use the **match** clauses of route maps to selectively suppress some more-specific routes of the aggregate and leave others unsuppressed. IP access lists and autonomous system path access lists match clauses are supported.

Using the **advertise-map** keyword selects specific routes that will be used to build different components of the aggregate route, such as AS_SET or community. This form of the **aggregate-address** command is useful when the components of an aggregate are in separate autonomous systems and you want to create an aggregate with AS_SET, and advertise it back to some of the same autonomous systems. You must remember to omit the specific autonomous system numbers from the AS_SET to prevent the aggregate from being dropped by the BGP loop detection mechanism at the receiving router. IP access lists and autonomous system path access lists **match** clauses are supported.

Using the **attribute-map** keyword allows attributes of the aggregate route to be changed. This form of the **aggregate-address** command is useful when one of the routes forming the AS_SET is configured with an attribute such as the community no-export attribute, which would prevent the aggregate route from being exported. An attribute map route map can be created to change the aggregate attributes.

Examples

AS-Set Example

In the following example, an aggregate BGP address is created in router configuration mode. The path advertised for this route will be an AS_SET consisting of all elements contained in all paths that are being summarized.

```
Router(config)# router bgp 50000
Router(config-router)# aggregate-address 10.0.0.0 255.0.0.0 as-set
```

Summary-Only Example

In the following example, an aggregate BGP address is created in address family configuration mode and applied to the multicast database under the IP Version 4 address family. Because the **summary-only** keyword is configured, more-specific routes are filtered from updates.

```
Router(config)# router bgp 50000
Router(config-router)# address-family ipv4 multicast
Router(config-router-af)# aggregate-address 10.0.0.0 255.0.0.0 summary-only
```

Conditional Aggregation Example

In the following example, a route map called MAP-ONE is created to match on an AS-path access list. The path advertised for this route will be an AS_SET consisting of elements contained in paths that are matched in the route map.

```
Router(config)# ip as-path access-list 1 deny ^1234_
Router(config)# ip as-path access-list 1 permit .*
Router(config)# !
Router(config)# route-map MAP-ONE
Router(config-route-map)# match ip as-path 1
Router(config-route-map)# exit
Router(config)# router bgp 50000
Router(config-router)# address-family ipv4
Router(config-router-af)# aggregate-address 10.0.0.0 255.0.0.0 as-set advertise-map
MAP-ONE
Router(config-router-af)# end
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
ip as-path access-list	Defines a BGP autonomous system path access list.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
neighbor distribute-list	Distributes BGP neighbor information in an access list.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.

allow-connections

To allow connections between specific types of endpoints in a VoIP network, use the **allow-connections** command in voice service configuration mode. To refuse specific types of connections, use the **no** form of this command.

allow-connections *from-type* **to** *to-type*

no allow-connections *from-type* **to** *to-type*

Syntax Description

from-type	Originating endpoint type. The following choices are valid: • **h323**—H.323. • **sip**—Session Interface Protocol (SIP).
to	Indicates that the argument that follows is the connection target.
to-type	Terminating endpoint type. The following choices are valid: • **h323**—H.323. • **sip**—Session Interface Protocol (SIP).

Command Default

Cisco IOS Release 12.3(4)T, Cisco IOS Release 12.3, and Earlier Releases

H.323-to-H.323 connections are enabled by default and cannot be changed, and POTS-to-any and any-to-POTS connections are disabled.

Cisco IOS Release 12.3(7)T and Later Releases

H.323-to-H.323 connections are disabled by default and can be changed, and POTS-to-any and any-to-POTS connections are enabled.

H.323-to-SIP Connections

H.323-to-SIP and SIP-to-H.323 connections are disabled by default, and POTS-to-any and any-to-POTS connections are enabled.

SIP-to-SIP Connections

SIP-to-SIP connections are disabled by default, and POTS-to-any and any-to-POTS connections are enabled.

Command Modes

Voice-service configuration (config-voi-serv)

Command History

Cisco IOS Release	Modification
12.2(13)T3	This command was introduced.
12.3(7)T	The default was changed.
12.3(11)T	The **sip** endpoint option was introduced for use with Cisco CallManager Express.

Cisco IOS Release	Modification
12.2(13)T3	This command was introduced.
12.4(4)T	This command was modified. The **sip** endpoint option was implemented for use in IP-to-IP gateway networks.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.4(22)T	Support for IPv6 was added.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

Cisco IOS Release 12.3(4)T, Cisco IOS Release 12.3, and Earlier Releases

This command is used to allow connections between specific types of endpoints in a Cisco multiservice IP-to-IP gateway. The command is enabled by default and cannot be changed. Connections to or from POTS endpoints are not allowed. Only H.323-to-H.323 connections are allowed.

Cisco IOS Release 12.3(7)T and Later Releases

This command is used with Cisco Unified Communications Manager Express 3.1 or later systems and with the Cisco Multiservice IP-to-IP Gateway feature. In Cisco Unified Communications Manager Express, the **allow-connections** command enables the VoIP-to-VoIP connections used for hairpin call routing or routing to an H.450 tandem gateway.

Examples

The following example specifies that connections between H.323 and SIP endpoints are allowed:

```
Router(config-voi-serv)# allow-connections h323 to sip
```

The following example specifies that connections between H.323 endpoints are allowed:

```
Router(config-voi-serv)# allow-connections h323 to h323
```

The following example specifies that connections between SIP endpoints are allowed:

```
Router(config-voi-serv)# allow-connections sip to sip
```

Related Commands

Command	Description
voice service	Enters voice service configuration mode.

anat

To enable Alternative Network Address Types (ANAT) on a Session Initiation Protocol (SIP) trunk, use the **anat** command in voice service SIP configuration mode or dial peer configuration mode. To disable ANAT on SIP trunks, use the **no** form of this command.

anat

no anat

Syntax Description

This command has no arguments or keywords.

Command Default

ANAT is enabled on SIP trunks.

Command Modes

Voice service voip-sip configuration (conf-serv-sip)
Dial peer configuration (config-dial-peer)

Command History

Release	Modification
12.4(22)T	This command was introduced.

Usage Guidelines

Both the Cisco IOS SIP gateway and the Cisco Unified Border Element are required to support Session Description Protocol (SDP) ANAT semantics for SIP IPv6 sessions. SDP ANAT semantics are intended to address scenarios that involve different network address families (for example, different IP versions). Media lines grouped using ANAT semantics provide alternative network addresses of different families for a single logical media stream. The entity creating a session description with an ANAT group must be ready to receive or send media over any of the grouped “m” lines.

By default, ANAT is enabled on SIP trunks. However, if the SIP gateway is configured in IPv4-only or IPv6-only mode, the gateway will not use ANAT semantics in its SDP offer.

Examples

The following example enables ANAT on a SIP trunk:

```
Router(conf-serv-sip)# anat
```

area (IPv6 address family configuration)

To configure Open Shortest Path First version 3 (OSPFv3) area parameters, use the **area** command in IPv6 address family configuration mode or IPv4 address family configuration mode. To remove this configuration, use the **no** form of this command.

area *area-ID* **range** *ipv6-prefix*/*prefix-length*

Syntax Description

area-ID	Area ID associated with the OSPFv3 interface.
range	Summarizes routes that match the address or address mask on border routers only.
ipv6-prefix/ *prefix-length*	An IPv6 prefix (address) and prefix length.
virtual-link	Defines a virtual link and its parameters. • This keyword can be used with the IPv6 address family only.
router-id	Router ID associated with the virtual-link neighbor. • This keyword can be used with the IPv6 address family only.

Command Default

This command is disabled by default.

Command Modes

IPv6 address family configuration (config-router-af)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

Use the **area** command in IPv6 or IPv4 address family configuration mode to configure OSPFv3 area parameters for an IPv6 or an IPv4 process.

Examples

The following example summarizes routes on the border router with the 2001:DB8:0:0::0/128 address:

```
Router(config-router)# address-family ipv6 unicast
Router(config-router-af)# area 1 range 2001:DB8:0:0::0/128
```

Related Commands

Command	Description
address-family ipv4	Enters IPv4 address family configuration mode for OSPFv3.

Command	Description
address-family ipv6	Enters IPv6 address family configuration mode for OSPFv3.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

area (OSPFv3 router configuration)

To configure the Open Shortest Path First version 3 (OSPFv3) area, use the **area** command in OSPFv3 router configuration mode. To remove this configuration, use the **no** form of this command.

area *area-ID* [**default-cost** | **nssa** | **stub**]

Syntax Description

default-cost	(Optional) Configures the cost for the default summary route used for a stub or not-so-stubby area (NSSA).
nssa	(Optional) Configures the NSSA.
stub	(Optional) Defines an area as a stub area.

Command Default

This command is not enabled by default.

Command Modes

OSPFv3 router configuration mode (config-router)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

Use the **area** command in OSPFv3 router configuration mode to configure OSPFv3 parameters for an IPv4 OSPFv3 process.

Examples

The following example configures OSPFv3 area 1:

```
Router(config-router)# area 1
```

Related Commands

Command	Description
address-family ipv4	Enters IPv4 address family configuration mode for OSPFv3.
address-family ipv6	Enters IPv6 address family configuration mode for OSPFv3.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

area authentication (IPv6)

To enable authentication for an Open Shortest Path First (OSPF) area, use the **area authentication** command in router configuration mode. To remove an authentication specification of an area or a specified area from the configuration, use the **no** form of this command.

area *area-id* **authentication ipsec spi** *spi* {**md5** | **sha1**} [*key-encryption-type*] *key*

no area *area-id* **authentication ipsec spi** *spi*

Syntax Description

area-id	Identifier of the area about which routes are to be summarized. It can be specified as either a decimal value or as an IPv6 prefix.
ipsec	IP Security (IPSec).
spi *spi*	Security policy index (SPI) value. The *spi* value must be a number from 256 to 4294967295, which is entered as a decimal.
md5	Enables Message Digest 5 (MD5) authentication on the area specified by the *area-id* argument.
sha1	Enables Secure Hash Algorithm 1 (SHA-1) authentication on the area specified by the *area-id* argument.
key-encryption-type	(Optional) Identifier of values that can be entered: • 0—The key is not encrypted. • 7—The key is encrypted.
key	Number used in the calculation of the message digest. The number is 32 hex digits (16 bytes) long.

Command Default

Key encryption type 0: key is not encrypted.

Command Modes

Router configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.4(4)T	The **sha1** keyword was added.

Usage Guidelines

Ensure that the same policy (the SPI and the key) is configured on all of the interfaces on the link. SPI values may be automatically used by other client applications, such as tunnels.

The policy database is common to all client applications on a box. This means that two IPSec clients, such as OSPF and a tunnel, cannot use the same SPI. Additionally, an SPI can only be used in one policy.

Beginning with Cisco IOS Release 12.4(4)T, the **sha-1** keyword can be used to choose SHA-1 authentication instead of entering the **md5** keyword to use MD5 authentication. The SHA-1 algorithm is considered to be somewhat more secure than the MD5 algorithm, and requires a 40 hex digit (20-byte) key rather than the 32 hex digit (16-byte) key that is required for MD5 authentication.

Examples

The following example enables authentication for the OSPF area 1:

```
area 1 authentication ipsec spi 678 md5 1234567890ABCDEF1234567890ABCDEF
```

The following example enables SHA-1 authentication for the OSPF area 0:

```
area 0 authentication ipsec spi 1000 sha1 1234567890123456789012345678901234567890
```

area encryption

To enable encryption for an Open Shortest Path First (OSPF) area, use the **area encryption** command in router configuration mode. To remove an encryption specification of an area or a specified area from the configuration, use the **no** form of this command.

area *area-id* **encryption ipsec spi** *spi* **esp** *encryption-algorithm* [[*key-encryption-type*] *key*] *authentication-algorithm* [*key-encryption-type*] *key*

no area *area-id* **encryption ipsec spi** *spi*

Syntax Description

area-id	Identifier of the area for which authentication is to be enabled. The identifier can be specified as either a decimal value or an IP address.
ipsec	IP Security (IPSec).
spi *spi*	Security policy index (SPI) value. The *spi* value must be a number from 256 to 4294967295.
esp	Encapsulating security payload (ESP).
encryption-algorithm	Encryption algorithm to be used with ESP. The values can be any of the following: • **aes-cdc**—Enables AES-CDC encryption • **3des**—Enables 3DES encryption • **des**—Enables DES encryption • **null**—ESP with no encryption.
key-encryption-type	(Optional) Identifier of values that can be entered: • **0**—The key is not encrypted. • **7**—The key is encrypted.
key	(Optional) Number used in the calculation of the message digest. The number is 32 hex digits (16 bytes) long. The size of the key depends on the encryption algorithm used. Some algorithms, such as AES-CDC, allow the user to choose the size of the key.
authentication-algorithm	Encryption authentication algorithm to be used. The values can be one of the following: • **md5**—Enables Message Digest 5 (MD5). • **sha-1**—Enables SHA-1.

Command Default

Authentication and encryption are not enabled.

Command Modes

Router configuration

Command History

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

Usage Guidelines

When the **area encryption** command is enabled, both authentication and encryption are enabled. However, when you use an **encryption** command such as **area encryption**, you may not also use an authentication command (such as **area authentication** or **area virtual-link authentication**) at the same time.

In IPv6, security is implemented using two IPv6 extension headers—the authentication header (AH) and ESP header. AH is used to provide connectionless integrity and data origin authentication for IPv6 datagrams, whereas ESP is used to provide confidentiality, connectionless integrity, data origin authentication, an antireplay service, and limited traffic flow confidentiality.

In OSPF for IPv6, authentication fields have been removed from OSPF packet headers. OSPF for IPv6 relies on the IPv6 extension headers, AH and ESP, to ensure integrity, authentication, and confidentiality of routing exchanges.

Examples

The following example provides ESP with no encryption and enables MD5 authentication on OSPF area 1:

```
Router(config-rtr)# area 1 encryption ipsec spi 500 esp null md5
1aaa2bbb3ccc4ddd5eee6fff7aaa8bbb
```

Related Commands

Command	Description
area authentication	Enables authentication for an OSPF area.
area virtual-link authentication	Enables authentication for virtual links in an OSPF area.
area virtual-link encryption	Enables encryption for virtual links in an OSPF area.
ipv6 ospf encryption	Specifies the encryption type for an interface.

area range

To consolidate and summarize routes at an area boundary, use the **area range** command in router configuration mode. To disable this function, use the **no** form of this command.

area *area-id* **range** *ipv6-prefix* /*prefix-length* [**advertise** | **not-advertise**] [**cost** *cost*]

no area *area-id* **range** *ipv6-prefix* /*prefix-length* [**advertise** | **not-advertise**] [**cost** *cost*]

Syntax Description

area-id	Identifier of the area about which routes are to be summarized. It can be specified as either a decimal value or as an IPv6 prefix.
ipv6-prefix	IPv6 prefix.
/*prefix-length*	IPv6 prefix length.
advertise	(Optional) Sets the address range status to advertise and generates a Type 3 summary link-state advertisement (LSA).
not-advertise	(Optional) Sets the address range status to DoNotAdvertise. The Type 3 summary LSA is suppressed, and the component networks remain hidden from other networks.
cost *cost*	(Optional) Metric or cost for this summary route, which is used during OSPF SPF calculation to determine the shortest paths to the destination. The value can be 0 to 16777215.

Command Default

This command is disabled by default.

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(24)S	Support for IPv6 was added. The **cost** keyword and *cost* argument were added.
12.2(15)T	Support for IPv6 was added. The **cost** keyword and *cost* argument were added.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
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.
12.2(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 introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The **area range** command is used only with Area Border Routers (ABRs). It is used to consolidate or summarize routes for an area. The result is that a single summary route is advertised to other areas by the ABR. Routing information is condensed at area boundaries. External to the area, a single route is advertised for each address range. This behavior is called *route summarization*.

Multiple **area** router configuration commands specifying the **range** option can be configured. Thus, OSPF can summarize addresses for many different sets of address ranges.

This command has been modified for Open Shortest Path First (OSPF) for IPv6. Users can now enter the IPv6 address syntax.

Note To remove the specified area from the software configuration, use the **no area** *area-id* command (with no other keywords). That is, the **no area** *area-id* command removes all area options, such as **area default-cost**, **area nssa**, **area range**, **area stub**, and **area virtual-link**.

Examples

The following example specifies one summary route to be advertised by the ABR to other areas for all subnets on network 10.0.0.0 and for all hosts on network 192.168.110.0:

```
interface Ethernet0/0
 no ip address
 ipv6 enable
 ipv6 ospf 1 area 1
!
ipv6 router ospf 1
 router-id 192.168.255.5
 log-adjacency-changes
 area 1 range 2001:0DB8:0:1::/64
```

The following example shows the IPv6 address syntax:

```
Router(config-rtr)# area 1 range ?

 X:X:X:X::X/<0-128>  IPv6 prefix x:x::y/z
```

area range

To consolidate and summarize routes at an area boundary, use the **area range** command in router address family topology or router configuration mode. To disable this function, use the **no** form of this command.

area *area-id* **range** *ip-address ip-address-mask* [**advertise | not-advertise**] [**cost** *cost*]

no area *area-id* **range** *ip-address ip-address-mask* [**advertise | not-advertise**] [**cost** *cost*]

Syntax Description

area-id	Identifier of the area for which routes are to be summarized. It can be specified as either a decimal value or an IPv6 prefix.
ip-address	IP address.
ip-address-mask	IP address mask.
advertise	(Optional) Sets the address range status to advertise and generates a Type 3 summary link-state advertisement (LSA).
not-advertise	(Optional) Sets the address range status to DoNotAdvertise. The Type 3 summary LSA is suppressed, and the component networks remain hidden from other networks.
cost *cost*	(Optional) Metric or cost for this summary route, which is used during OSPF SPF calculation to determine the shortest paths to the destination. The value can be 0 to 16777215.

Command Default

This command is disabled by default.

Command Modes

Router address family topology configuration (config-router-af-topology)
Router configuration (config-router)

Command History

Release	Modification
10.0	This command was introduced.
12.0(24)S	The **cost** keyword and *cost* argument were added.
12.2(15)T	The **cost** keyword and *cost* argument were added.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)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	This command was made available in router address family topology configuration mode.
12.2SX	This command is supported in the Cisco 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 **area range** command is used only with Area Border Routers (ABRs). It is used to consolidate or summarize routes for an area. The result is that a single summary route is advertised to other areas by the ABR. Routing information is condensed at area boundaries. External to the area, a single route is advertised for each address range. This behavior is called *route summarization*.

Multiple **area range** router configuration commands can be configured. Thus, OSPF can summarize addresses for many different sets of address ranges.

Note To remove the specified area from the software configuration, use the **no area** *area-id* command (with no other keywords). That is, the **no area** *area-id* command removes all area options, such as **area default-cost**, **area nssa**, **area range**, **area stub**, and **area virtual-link**.

Release 12.2(33)SRB

If you plan to configure the Multi-Topology Routing (MTR) feature, you need to enter the **area range** command in router address family topology configuration mode in order for this OSPF router configuration command to become topology-aware.

Examples

The following example specifies one summary route to be advertised by the ABR to other areas for all subnets on network 10.0.0.0 and for all hosts on network 192.168.110.0:

```
interface ethernet 0
 ip address 192.168.110.201 255.255.255.0
!
interface ethernet 1
 ip address 192.168.120.201 255.255.255.0
!
router ospf 201
 network 192.168.110.0 0.0.0.255 area 0
 area 10.0.0.0 range 10.0.0.0 255.0.0.0
 area 0 range 192.168.110.0 255.255.0.0
```

Related Commands

Command	Description
area range (IPv6)	Consolidates and summarizes routes at an area boundary in an IPv6 network.

area virtual-link

To define an Open Shortest Path First (OSPF) virtual link, use the **area virtual-link** command in router address family topology or router configuration mode. To remove a virtual link, use the **no** form of this command.

area *area-id* **virtual-link** *router-id* [**hello-interval** *seconds*] [**retransmit-interval** *seconds*] [**transmit-delay** *seconds*] [**dead-interval** *seconds*] [**ttl-security hops** *hop-count*]

no area *area-id* **virtual-link** *router-id*

Syntax Description

area-id	Area ID assigned to the virtual link. This can be either a decimal value or a valid IPv6 prefix. There is no default.
router-id	Router ID associated with the virtual link neighbor. The router ID appears in the **show ip ospf** or **show ipv6 display** command. There is no default.
hello-interval *seconds*	(Optional) Specifies the time (in seconds) between the hello packets that the Cisco IOS software sends on an interface. The hello interval is an unsigned integer value to be advertised in the hello packets. The value must be the same for all routers and access servers attached to a common network. Range is from 1 to 8192. The default is 10.
retransmit-interval *seconds*	(Optional) Specifies the time (in seconds) between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface. The retransmit interval is the expected round-trip delay between any two routers on the attached network. The value must be greater than the expected round-trip delay. Range is from 1 to 8192. The default is 5.
transmit-delay *seconds*	(Optional) Specifies the estimated time (in seconds) required to send a link-state update packet on the interface. The integer value that must be greater than zero. LSAs in the update packet have their age incremented by this amount before transmission. Range is from 1 to 8192. The default value is 1.
dead-interval *seconds*	(Optional) Specifies the time (in seconds) that hello packets are not seen before a neighbor declares the router down. The dead interval is an unsigned integer value. The default is four times the hello interval, or 40 seconds. As with the hello interval, this value must be the same for all routers and access servers attached to a common network.
ttl-security hops *hop-count*	(Optional) Configures Time-to-Live (TTL) security on a virtual link. The *hop-count* argument range is from 1 to 254.

Command Default

No OSPF virtual link is defined.

Command Modes

Router address family topology configuration (config-router-af-topology)
Router configuration (config-router)

Command History

Release	Modification
10.0	This command was introduced.
12.0(24)S	Support for IPv6 was added.
12.2(15)T	Support for IPv6 was added.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)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	This command was made available in router address family topology configuration mode.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SRC	The **ttl-security hops** *hop-count* keywords and argument were added.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

In OSPF, all areas must be connected to a backbone area. If the connection to the backbone is lost, it can be repaired by establishing a virtual link.

The smaller the hello interval, the faster topological changes will be detected, but more routing traffic will ensue. The setting of the retransmit interval should be conservative, or needless retransmissions will result. The value should be larger for serial lines and virtual links.

The transmit delay value should take into account the transmission and propagation delays for the interface.

To configure a virtual link in OSPF for IPv6, you must use a router ID instead of an address. In OSPF for IPv6, the virtual link takes the router ID rather than the IPv6 prefix of the remote router.

Use the **ttl-security hops** *hop-count* keywords and argument to enable checking of TTL values on OSPF packets from neighbors or to set TTL values sent to neighbors. This feature adds an extra layer of protection to OSPF.

Note In order for a virtual link to be properly configured, each virtual link neighbor must include the transit area ID and the corresponding virtual link neighbor router ID. To see the router ID, use the **show ip ospf** or the **show ipv6 ospf** command in privileged EXEC mode.

Note To remove the specified area from the software configuration, use the **no area** *area-id* command (with no other keywords). That is, the **no area** *area-id* command removes all area options, such as **area default-cost**, **area nssa**, **area range**, **area stub**, and **area virtual-link**.

Release 12.2(33)SRB

If you plan to configure the Multi-Topology Routing (MTR) feature, you need to enter the **area virtual-link** command in router address family topology configuration mode in order for this OSPF router configuration command to become topology-aware.

Examples

The following example establishes a virtual link with default values for all optional parameters:

```
ipv6 router ospf 1
 log-adjacency-changes
 area 1 virtual-link 192.168.255.1
```

The following example establishes a virtual link in OSPF for IPv6:

```
ipv6 router ospf 1
 log-adjacency-changes
 area 1 virtual-link 192.168.255.1 hello-interval 5
```

Related Commands

Command	Description
ttl-security hops	Enables checking of TTL values on OSPF packets from neighbors or setting TTL values sent to neighbors.
show ip ospf	Enables the display of general information about Open Shortest Path First (OSPF) routing processes.
show ipv6 ospf	Enables the display of general information about Open Shortest Path First (OSPF) routing processes.

area virtual-link authentication

To enable authentication for virtual links in an Open Shortest Path First (OSPF) area, use the **area virtual-link authentication** command in router configuration mode. To remove authentication from an area, use the **no** form of this command.

area *area-id* **virtual-link** *router-id* [**hello-interval** *seconds*] [**retransmit-interval** *seconds*] [**transmit-delay** *seconds*] [**dead-interval** *seconds*] **authentication ipsec spi** *spi authentication-algorithm* [*key-encryption-type*] *key*

no area *area-id* **virtual-link** *router-id* **authentication ipsec spi** *spi*

Syntax Description

area-id	Identifier of the area assigned to the transit area for the virtual link. This can be either a decimal value or a valid IPv6 prefix. There is no default.
router-id	Router ID associated with the virtual link neighbor. The router ID appears in the **show ipv6 ospf** display. There is no default.
hello-interval *seconds*	(Optional) Time (in seconds) between the hello packets that the Cisco IOS software sends on an interface. The hello interval is an unsigned integer value to be advertised in the hello packets. The value must be the same for all routers and access servers attached to a common network. The default is 10 seconds.
retransmit-interval *seconds*	(Optional) Time (in seconds) between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface. The retransmit interval is the expected round-trip delay between any two routers on the attached network. The value must be greater than the expected round-trip delay. The default is 5 seconds.
transmit-delay *seconds*	(Optional) Estimated time (in seconds) required to send a link-state update packet on the interface. The integer value that must be greater than zero. LSAs in the update packet have their age incremented by this amount before transmission. The default value is 1 second.
dead-interval *seconds*	(Optional) Time (in seconds) that hello packets are not seen before a neighbor declares the router down. The dead interval is an unsigned integer value. The default is four times the hello interval, or 40 seconds. As with the hello interval, this value must be the same for all routers and access servers attached to a common network.
ipsec	IP Security (IPSec).
spi *spi*	Security policy index (SPI) value. The *spi* value must be a number from 256 to 4294967295.
authentication-algorithm	Encryption authentication algorithm to be used. The values can be one of the following: • **md5**—Enables Message Digest 5 (MD5). • **sha-1**—Enables SHA-1.

key-encryption-type	(Optional) Identifier of values that can be entered: • **0**—The key is not encrypted. • **7**—The key is encrypted.
key	Number used in the calculation of the message digest. The number is 32 hex digits (16 bytes) long. The size of the key depends on the encryption algorithm used. Some algorithms, such as AES-CDC, allow the user to choose the size of the key.

Command Default

Authentication is not enabled on an area.
area-id: No area ID is predefined.
router-id: No router ID is predefined.
hello-interval *seconds*: 10 seconds
retransmit-interval *seconds*: 5 seconds
transmit-delay *seconds*: 1 second
dead-interval *seconds*: 40 seconds

Command Modes

Router configuration

Command History

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

Usage Guidelines

When you use an **encryption** command such as **area encryption**, you may not also use an authentication command (such as **area authentication** or **area virtual-link authentication**) at the same time.

In OSPF, all areas must be connected to a backbone area. If the connection to the backbone is lost, it can be repaired by establishing a virtual link.

To configure a virtual link in OSPF for IPv6, you must use a router ID instead of an address. In OSPF for IPv6, the virtual link takes the router ID rather than the IPv6 prefix of the remote router.

Examples

The following example enables authentication for virtual links in OSPF area 1. The router ID associated with the virtual link neighbor is 10.0.0.1, the IPSec SPI value is 940, and the authentication algorithm used is MD5:

```
Router(config)# ipv6 router ospf 1
Router(config-rtr)# area 1 virtual-link 10.0.0.1 authentication ipsec spi 940 md5
1234567890ABCDEF1234567890ABCDEF
```

Related Commands

Command	Description
area authentication	Enables authentication for an OSPF area.
area encryption	Enables encryption for an OSPF area.

area virtual-link encryption

To enable encryption for virtual links in an Open Shortest Path First (OSPF) area, use the **area virtual-link encryption** command in router configuration mode. To remove encryption from an area, use the **no** form of this command.

area *area-id* **virtual-link** *router-id* [**hello-interval** *seconds*] [**retransmit-interval** *seconds*] [**transmit-delay** *seconds*] [**dead-interval** *seconds*] **encryption ipsec spi** *spi* **esp** *encryption-algorithm* [[*key-encryption-type*] *key*] *authentication-algorithm* [*key-encryption-type*] *key*

no area *area-id* **virtual-link** *router-id* **encryption ipsec spi** *spi*

Syntax Description

area-id	Identifier of the area assigned to the area for the virtual link. This can be either a decimal value or a valid IPv6 prefix. There is no default.
router-id	Router ID associated with the virtual link neighbor. There is no default.
hello-interval *seconds*	(Optional) Time (in seconds) between the hello packets that the Cisco IOS software sends on an interface. The hello interval is an unsigned integer value to be advertised in the hello packets. The value must be the same for all routers and access servers attached to a common network. The default is 10 seconds.
retransmit-interval *seconds*	(Optional) Time (in seconds) between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface. The retransmit interval is the expected round-trip delay between any two routers on the attached network. The value must be greater than the expected round-trip delay. The default is 5 seconds.
transmit-delay *seconds*	(Optional) Estimated time (in seconds) required to send a link-state update packet on the interface. The integer value that must be greater than zero. LSAs in the update packet have their age incremented by this amount before transmission. The default value is 1 second.
dead-interval *seconds*	(Optional) Time (in seconds) that hello packets are not seen before a neighbor declares the router down. The dead interval is an unsigned integer value. The default is four times the hello interval, or 40 seconds. As with the hello interval, this value must be the same for all routers and access servers attached to a common network.
ipsec	IP Security (IPSec).
spi *spi*	Security policy index (SPI) value. The *spi* value must be a number from 256 to 4294967295.
esp	Encapsulating security payload (ESP).
encryption-algorithm	Encryption algorithm to be used with ESP. The values can be any of the following: • **aes-cdc**—Enables AES-CDC encryption. • **3des**—Enables 3DES encryption. • **des**—Enables DES encryption. • **null**—ESP with no encryption.

key-encryption-type	(Optional) Identifier of values that can be entered: • **0**—The key is not encrypted. • **7**—The key is encrypted.
key	Number used in the calculation of the message digest. The number is 32 hex digits (16 bytes) long. The size of the key depends on the encryption algorithm used. Some algorithms, such as AES-CDC, allow the user to choose the size of the key.
authentication-algorithm	Encryption authentication algorithm to be used. The values can be one of the following: • **md5**—Enables Message Digest 5 (MD5). • **sha1**—Enables SHA-1.

Command Default

Authentication and encryption are not enabled.
area-id: No area ID is predefined.
router-id: No router ID is predefined.
hello-interval *seconds*: 10 seconds
retransmit-interval *seconds*: 5 seconds
transmit-delay *seconds*: 1 second
dead-interval *seconds*: 40 seconds

Command Modes

Router configuration

Command History

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

Usage Guidelines

When the **area virtual-link encryption** command is enabled, both authentication and encryption are enabled. However, when you use an **encryption** command such as **area encryption**, you may not also use an authentication command (such as **area authentication** or **area virtual-link authentication**) at the same time.

Interface-level configuration takes precedence over an area configuration. If the interface configuration is removed, then an area configuration is applied to the interface. Authentication and encryption may be configured at the same time.

Examples

The following example enables encryption for virtual links in OSPF area 1. The router ID associated with the virtual link neighbor is 10.1.0.1, the IPSec SPI value is 3944, and the encryption algorithm used is SHA-1:

```
Router(config)# ipv6 router ospf 1
Router(config-rtr)# area 1 virtual-link 10.1.0.1 hello-interval 2 dead-interval 10
encryption ipsec spi 3944 esp null sha1 123456789A123456789B123456789C123456789D
```

Related Commands

Command	Description
area authentication	Enables authentication for an OSPF area.
area encryption	Enables encryption for an OSPF area.
area virtual-link authentication	Enables authentication for virtual links in an OSPF area.

arp (interface)

To support a type of encapsulation for a specific network, such as Ethernet, Fiber Distributed Data Interface (FDDI), Frame Relay, and Token Ring, so that the 48-bit Media Access Control (MAC) address can be matched to a corresponding 32-bit IP address for address resolution, use the **arp** command in interface configuration mode. To disable an encapsulation type, use the **no** form of this command.

arp {**arpa** | **frame-relay** | **snap**}

no arp {**arpa** | **frame-relay** | **snap**}

Syntax Description

arpa	Standard Ethernet-style Address Resolution Protocol (ARP) (RFC 826).
frame-relay	Enables ARP over a Frame Relay encapsulated interface.
snap	ARP packets conforming to RFC 1042.

Defaults

Standard Ethernet-style ARP

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(13)T	The **probe** keyword was removed because the HP Probe feature 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.
12.0(33)S	Support for IPv6 was added. This command was implemented on the Cisco 12000 series routers.

Usage Guidelines

Unlike most commands that have multiple arguments, the **arp** command has arguments that are not mutually exclusive. Each command enables or disables a specific type of encapsulation.

Given a network protocol address (IP address), the **arp frame-relay** command determines the corresponding hardware address, which would be a data-link connection identifier (DLCI) for Frame Relay.

The **show interfaces** command displays the type of encapsulation being used on a particular interface. To remove all nonstatic entries from the ARP cache, use the **clear arp-cache** command.

Examples

The following example enables Frame Relay services:

```
interface ethernet 0
 arp frame-relay
```

Related Commands

Command	Description
clear arp-cache	Deletes all dynamic entries from the ARP cache.
show interfaces	Displays statistics for all interfaces configured on the router or access server.

associate application

To associate an application to the digital signal processor (DSP) farm profile, use the **associate application** command in DSP farm profile configuration mode. To remove the protocol, use the **no** form of this command.

associate application {**cube** | **sbc** | **sccp**} *profile-description-text*

no associate application sccp

Syntax Description

cube	Associates the Cisco Unified Border Element application to a defined profile in the DSP farm.
sbc	Associates the SBC application to a defined profile in the DSP farm.
sccp	Associates the skinny client control protocol application to a defined profile in the DSP farm.
profile-description-text	(Optional) User defined name for the associated application.

Command Default

No application is associated with the DSP farm profile.

Command Modes

DSP farm profile configuration (config-dspfarm-profile)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.4(22)T	Support for IPv6 was added.
Cisco IOS XE Release 3.2S	This command was modified. The **cube** and **sbc** keywords and the *profile-description-text* argument were added.

Usage Guidelines

Use the associate application command to associate an application to a predefined DSP farm profile.

Examples

The following example associates SCCP to the DSP farm profile:

```
Router(config-dspfarm-profile)# associate application sccp
```

The following example associates Cisco Unified Border Element to the DSP farm profile:

```
Router(config-dspfarm-profile)# associate application cube
```

Related Commands

Command	Description
voice-card	Enters voice card configuration mode
codec (dspfarm-profile)	Specifies the codecs supported by a DSP farm profile.
description (dspfarm-profile)	Includes a specific description about the DSP farm profile.
dspfarm profile	Enters DSP farm profile configuration mode and defines a profile for DSP farm services.
maximum sessions (dspfarm-profile)	Specifies the maximum number of sessions that need to be supported by the profile.
shutdown (dspfarm-profile)	Allocates DSP farm resources and associates with the application.

associate profile

To associate a digital signal processor (DSP) farm profile with a Cisco CallManager group, use the **associate profile** command in SCCP Cisco CallManager configuration mode. To disassociate a DSP farm profile from a Cisco Unified CallManager, use the **no** form of this command.

associate profile *profile-identifier* **register** *device-name*

no associate profile *profile-identifier* **register** *device-name*

Syntax Description

profile-identifier	Number that identifies the DSP farm profile. Range is 1 to 65535. There is no default value.
register *device-name*	User-specified device name in Cisco Unified CallManager. A maximum number of 15 characters can be entered for the device name.

Command Default

This command is not enabled.

Command Modes

SCCP Cisco CallManager configuration (config-sccp-ccm)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4(22)T	Support for IPv6 was added.

Usage Guidelines

The device name must match the name configured in Cisco UnifiedCallManager; otherwise the profile is not registered to Cisco Unified CallManager.

Note Each profile can be associated to only one Cisco CallManager group.

Examples

The following example associates DSP farm profile abgz12345 to Cisco CallManager group 999:

```
Router(config)# sccp ccm group 999
Router(config-sccp-ccm)# associate profile 1 register abgz12345
```

Related Commands

Command	Description
bind interface	Binds an interface to a Cisco CallManager group.
dspfarm profile	Enters DSP farm profile configuration mode and defines a profile for DSP farm services.
sccp ccm group	Creates a Cisco CallManager group and enters SCCP Cisco CallManager configuration mode.

atm pppatm passive

To place an ATM subinterface in passive mode, use the **atm pppatm passive** command in ATM subinterface configuration mode. To change the configuration back to the default (active) mode, use the **no** form of this command.

atm pppatm passive

no atm pppatm passive

Syntax Description

This command has no arguments or keywords.

Defaults

Active mode

Command Modes

ATM subinterface 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.

Usage Guidelines

The **atm pppatm passive** command places PPP over ATM (PPPoA) sessions on an ATM subinterface in "listening" mode. Rather than trying to establish the sessions actively by sending out Link Control Protocol (LCP) packets, these sessions listen to the incoming LCP packets and become active only after they have received their first LCP packet. This feature is useful for L2TP access concentrators (LACs) in the broadband access deployments where thousands of PPPoA sessions are configured on LACs. When PPPoA is in the passive mode, the LAC brings up the sessions only when the subscribers become active and not use its processing power on polling all sessions.

For better scalability and faster convergence of PPP sessions, you should set the PPPoA sessions to passive mode at the LAC.

Cisco 10000 Series Router

For better scalability and faster convergence of PPPoA, PPP over Ethernet over ATM (PPPoEoA), or LAC sessions, set the sessions to passive mode.

You must use the a**tm pppatm passive** command for large-scale PPP terminated aggregation (PPPoA and PPPoEoA) and Layer 2 Tunnel Protocol (L2TP) access concentrator (LAC). Instead of sending out LCP packets to establish the sessions actively, the sessions listen to the incoming LCP packets and become active only after they receive their first LCP packet. When PPPoX is in the passive mode, the LAC brings up the sessions only when the subscribers become active and does not use processing power polling all sessions.

Examples

The following example configures the passive mode for the PPPoA sessions on an ATM subinterface:

```
Router(config)# interface atm 1/0.1 multipoint
Router(config-subif)# atm pppatm passive
Router(config-subif)# range range-pppoa-1 pvc 100 199
Router(config-subif-atm-range)# protocol ppp virtual-template 1
```

Cisco 10000 Series Router

The following example configures passive mode for the PPPoA sessions on an ATM multipoint subinterface:

```
Router(config)# interface atm 1/0.1 multipoint
Router(config-subif)# atm pppatm passive
Router(config-subif)# range range-pppoa-1 pvc 100 199
Router(config-subif-atm-range)# encapsulation aal5mux ppp virtual-template 1
```

atm route-bridged

To configure an interface to use the ATM routed bridge encapsulation (RBE), use the **atm route-bridged** command in interface configuration mode.

atm route-bridged *protocol*

Syntax Description

protocol	Protocol to be route-bridged. IP and IPv6 are the only protocols that can be route-bridged using ATM RBE.

Command Default

ATM routed bridge encapsulation is not configured.

Command Modes

ATM subinterface configuration

Command History

Release	Modification
12.0(5)DC	This command was introduced.
12.1(2)T	This command was integrated in Cisco IOS Release 12.1(2)T.
12.3(4)T	The **ipv6** keyword was added to support RBE of IPv6 packets as specified in RFC 1483.
12.4(2)T	This command was updated to work with QoS policy-based routing in Cisco IOS Release 12.4(2)T.
Cisco IOS XE Release 3.2S	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

Use this command to configure RBE on an ATM interface. The **atm route-bridged** command can also be used to integrate RBE with quality of service (QoS) features on the Cisco 800 and 1700 series routers.

Routing of IPv6 and IP Packets

IP and IPv6 packets can be routed using RBE only over ATM point-to-point subinterfaces.

Routing of IP packets and IPv6 half-bridging, bridging, PPP over Ethernet (PPPoE), or other Ethernet 802.3-encapsulated protocols can be configured on the same subinterface.

Router Advertisements with IPv6

Router advertisements are suppressed by default. For stateless autoconfiguration, router advertisements must be allowed with the **no ipv6 nd suppress-ra** command. For static configuration, router advertisement is not required; however, the aggregator should either have the RBE interface on the same subnet as the client or have a static IPv6 route to that subnet through the RBE interface.

Examples

IP Encapsulation Example

The following example configures ATM routed bridge encapsulation on an interface:

```
interface atm 4/0.100 point-to-point
 ip address 172.16.5.9 255.255.255.0
 atm route-bridged ip
 pvc 0/32
```

IPv6 Encapsulation Example

The following example shows a typical configuration on an RBE interface to allow routing of IPv6 encapsulated Ethernet packets. IPv6 packets sent out of the subinterface are encapsulated over Ethernet over the RBE interface.

```
interface ATM1/0.1 point-to-point
 ipv6 enable
 ipv6 address 3FEE:12E1:2AC1:EA32::/64
 no ipv6 nd suppress-ra
 atm route-bridged ipv6
 pvc 1/101
```

In this example, the **ipv6 enable** command allows the routing of IPv6 packets. The **ipv6 address** command specifies an IPv6 address for the interface and an IPv6 prefix to be advertised to a peer. The **no ipv6 nd ra suppress** command enables router advertisements on the interface.

IPv6 Routing and Bridging of Other Traffic Example

The following example shows a configuration in which IPv6 packets are routed and all other packets are bridged.

```
interface ATM1/0.1 point-to-point
 ipv6 enable
 ipv6 address 3FEE:12E1:2AC1:EA32::/64
 atm route-bridged ipv6
 bridge-group 1
 pvc 1/101
```

IP and IPv6 Routing with Bridging of Other Protocols Example

IP and IPv6 routing can be configured on the same interface as shown in this example. All other packets are bridged. PPPoE could also be configured on this same interface.

```
interface ATM1/0.1 point-to-point
 ipv6 enable
 ipv6 address 3FEE:12E1:2AC1:EA32::/64
 ip address 10.0.0.1 255.255.255.0
 atm route-bridged ipv6
 atm route-bridged ip
 bridge-group 1
 pvc 1/101
```

Static Configuration Example

The following example shows the IPv6 static route configured. Unlike IP, the IPv6 interface on an aggregator is always numbered and, minimally, has a link local IPv6 address.

```
Router# configure terminal
Router(config)# ipv6 route 3FEE:12E1:2AC1:EA32::/64 atm1/0.3
Router(config)# end
```

show ipv6 interface Example

Notice in this **show ipv6 interface** output display that each RBE link has its own subnet prefix. Unlike proxy ARP in IPv4 RBE configurations, the aggregator does not require proxy ND in IPv6 RBE deployments.

```
Router# show ipv6 interface atm1/0.1

ATM1/0.1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::203:FDFF:FE3B:B400
  Global unicast address(es):
    3FEE:12E1:2AC1:EA32::, subnet is 3FEE:12E1:2AC1:EA32::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:0
    FF02::1:FF3B:B400
  MTU is 4470 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses
```

Integrated Class-Based Weighted Fair Queueing and RBE on ATM Example

The following partial example configures a single PVC using AAL5SNAP encapsulation and class-based routing for traffic shaping on the interface where RBE is enabled. The following CBWFQ parameters are configured: access-list with different IP precedence, class map, policy map, and service policy. Different bandwidth classes are configured in the same policy.

RBE base configuration:

```
interface FastEthernet0
 ip address 172.22.1.1 255.255.0.0
!
interface ATM0.1 point-to-point
 ip address 10.1.1.5 255.255.255.252
 atm route-bridged ip
 pvc 88/800
  encapsulation aal5snap
!
interface ATM0.1 point-to-point
 ip address 10.1.1.1 255.255.255.252
 atm route-bridged ip
 pvc 99/900
  encapsulation aal5snap
!
interface ATM0.1 point-to-point
 ip address 172.18.0.1 255.0.0.0
 pvc 100/1000
!
router eigrp 100
 network 10.1.0.0
 network 172.18.0.0
 network 172.22.0.0
.
.
.
```

CBWFQ configuration:

```
class-map match-all voice
 match access-group 105
!
policy-map voicedatapolicy
 class voice
  bandwidth 200
 class class-default
  fair-queue
  random-detect
!
interface Ethernet0
 ip address 172.25.1.1 255.0.0.0
 hold-queue 600 in
 hold-queue 100 out
!
interface ATM0
 no ip address
 no atm ilmi-keepalive
 dsl operating-mode auto
!
interface ATM0.1 point-to-point
 ip address 10.2.3.4 255.255.255.0
 atm route-bridged ip
 pvc 1/42
  protocol ip 10.2.3.5 broadcast
  vbr-nrt 300 300
  encapsulation aal5snap
  service-policy output voicedatapolicy
.
.
.
```

Related Commands

Command	Description
no ipv6 nd ra suppress	Suppresses IPv6 router advertisement transmissions on a LAN interface.

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 (Mobile IPv6)

To specify the authentication properties for the IPv6 mobile node by creating either a unidirectional or bidirectional security parameter index (SPI), use the **authentication** command in home agent configuration mode or IPv6 mobile router host configuration mode. To remove these authentication properties, use the **no** form of this command.

authentication {**inbound-spi** {*hex-in* | **decimal** *decimal-in*} **outbound-spi** {*hex-out* | **decimal** *decimal-out*} | **spi** {*hex-value* | **decimal** *decimal-value*}} **key** {**ascii** *string* | **hex** *string*}[**algorithm** *algorithm-type*] [**replay within** *seconds*]

no authentication

Syntax Description

inbound-spi	Bidirectional SPI used to authenticate inbound registration packets.
hex-in	Index for inbound registration packets. The range is from 100 to ffffffff.
decimal *decimal-in*	SPI expressed as a decimal number for inbound registration packets. The range is from 256 to 4294967295.
outbound-spi	SPI used for calculating the authenticator in outbound registration packets.
hex-out	Index for outbound registration packets. The range is from 100 to ffffffff.
decimal *decimal-out*	SPI expressed as a decimal number. The range is from 256 to 4294967295.
spi	Unidirectional SPI used to authenticate a peer. **Note** Cisco recommends that you use hexadecimal values instead of decimal values for interoperability.
hex-value	SPI expressed as a hexadecimal number. The range is from 100 to ffffffff.
decimal *decimal-value*	SPI expressed as a decimal number. The range is from 256 to 4294967295.
key	Security key.
ascii *string*	Security key expressed as an ASCII string. A maximum of 32 characters is allowed. No spaces are allowed.
hex *string*	Security key expressed in hexadecimal digits. A maximum of 32 hex digits is allowed. The range is from 100 to ffffffff. No spaces are allowed.
algorithm	(Optional) Algorithm used to authenticate messages during registration.
algorithm-type	(Optional) Type of algorithm. The hash-based Message Authentication Code (HMAC)-SHA1 algorithm is used.
replay within	(Optional) Specifies the number of seconds that the router uses for replay protection.
seconds	(Optional) Time, in seconds, that a router uses for replay protection. The range is from plus or minus 255. The default is plus or minus 7. The registration packet is considered “not replayed” if the time stamp in the packet is within plus or minus the configured number of seconds of the router clock.

Command Default

No SPI is configured.

Command Modes Home agent configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.
12.4(20)T	IPv6 network mobility (NEMO) functionality was added.

Usage Guidelines The **authentication** command provides mobility message authentication by creating a mobility SPI, a key, an authentication algorithm, and a replay protection mechanism. Mobility message authentication option is used to authenticate binding update (BU) and binding acknowledgment (BA) messages based on the shared-key-based security association between the mobile node and the home agent.

The mobile node or home agent receiving this BU must verify the authentication data in the option. If authentication fails, the home agent must send a FAIL message. If the home agent does not have shared-key-based mobility SA, the home agent MUST discard the BU.

The mobility message replay protection option may be used in BU or BA messages when authenticated using the mobility message authentication option. The mobility message replay protection option, configured using the **replay within** keywords, is used to let the home agent verify that a BU has been freshly generated by the mobile node and not replayed by an attacker from some previous BU. This function is especially useful for cases in which the home agent does not maintain stateful information about the mobile node after the binding entry has been removed. The home agent performs the replay protection check after the BU has been authenticated. The mobility message replay protection option, when included, is used by the mobile node for matching the BA with the BU.

Examples The following example shows a unidirectional SPI and a key:

```
authentication spi 500 key ascii cisco
```

Related Commands

Command	Description
address (IPv6 mobile router)	Specifies the home address of the IPv6 mobile node,
host group	Creates a host configuration in IPv6 Mobile.
ipv6 mobile home-agent (global configuration)	Enters home agent configuration mode.
nai	Specifies the NAI for the IPv6 mobile node.

auto-cost (IPv6)

To control the reference value Open Shortest Path First version 3 (OSPF) uses when calculating metrics for interfaces in an IPv6 OSPFv3 process, use the **auto-cost** command in router configuration mode. To return the reference value to its default, use the **no** form of this command.

auto-cost reference-bandwidth *Mbps*

no auto-cost reference-bandwidth

Syntax Description

reference-bandwidth *Mbps*	Rate in Mbps (bandwidth). The range is from 1 to 4294967. The default is 100.

Command Default

The reference value is 100 Mbps.

Command Modes

Router 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.
15.1(3)S	Use of the **ospfv3 cost** command can affect the **ipv6 ospf cost** command.
Cisco IOS XE Release 3.4S	Use of the **ospfv3 cost** command can affect the **ipv6 ospf cost** command.
15.2(1)T	Use of the **ospfv3 cost** command can affect the **ipv6 ospf cost** command.

Usage Guidelines

The OSPF version 3 metric is calculated as the *Mbps* value divided by the bandwidth, with *Mbps* equal to 10^8 by default, and bandwidth determined by the **bandwidth** (interface) command. The calculation gives Fast Ethernet a metric of 1.

If you have multiple links with high bandwidth (such as Fast Ethernet or ATM), you might want to use a larger number to differentiate the cost on those links.

Using this formula, the default path costs were calculated as noted in the following bulleted list. If these values do not suit your network, you can use your own method of calculating path costs.

- 56-kbps serial link—Default cost is 1785.
- 64-kbps serial link—Default cost is 1562.
- T1 (1.544-Mbps serial link)—Default cost is 64.
- E1 (2.048-Mbps serial link)—Default cost is 48.
- 4-Mbps Token Ring—Default cost is 25.
- Ethernet—Default cost is 10.
- 16-Mbps Token Ring—Default cost is 6.

- Fast Ethernet—Default cost is 1.
- X25—Default cost is 5208.
- Asynchronous—Default cost is 10,000.
- ATM—Default cost is 1.

The value set by the **ospfv3 cost** or **ipv6 ospf cost** command overrides the cost resulting from the **auto-cost** command.

Examples

The following example sets the auto-cost reference bandwidth to 1000 Mbps:

```
ipv6 router ospf 1
 auto-cost reference-bandwidth 1000
```

Related Commands

Command	Description
ipv6 ospf cost	Explicitly specifies the cost of sending an IPv6 packet on an interface.
ospfv3 cost	Explicitly specifies the cost of sending a packet on an OSPFv3 interface.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

auto-cost (OSPFv3)

To control the reference value Open Shortest Path First version 3 (OSPFv3) uses when calculating metrics for interfaces in an IPv4 OSPFv3 process, use the **auto-cost** command in OSPFv3 router configuration mode. To return the reference value to its default, use the **no** form of this command.

auto-cost reference-bandwidth *Mbps*

no auto-cost reference-bandwidth

Syntax Description

reference-bandwidth *Mbps*	Rate in Mbps (bandwidth). The range is from 1 to 4294967. The default is 100.

Command Default

The reference value is 100 Mbps.

Command Modes

OSPFv3 router configuration mode (config-router)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

The OSPF version 3 metric is calculated as the *Mbps* value divided by the bandwidth, with *Mbps* equal to 10^8 by default, and bandwidth determined by the **bandwidth** (interface) command. The calculation gives Fast Ethernet a metric of 1.

If you have multiple links with high bandwidth (such as Fast Ethernet or ATM), you might want to use a larger number to differentiate the cost on those links.

Using this formula, the default path costs were calculated as noted in the following bulleted list. If these values do not suit your network, you can use your own method of calculating path costs.

- 56-kbps serial link—Default cost is 1785.
- 64-kbps serial link—Default cost is 1562.
- T1 (1.544-Mbps serial link)—Default cost is 64.
- E1 (2.048-Mbps serial link)—Default cost is 48.
- 4-Mbps Token Ring—Default cost is 25.
- Ethernet—Default cost is 10.
- 16-Mbps Token Ring—Default cost is 6.
- Fast Ethernet—Default cost is 1.
- X25—Default cost is 5208.

- Asynchronous—Default cost is 10,000.
- ATM—Default cost is 1.

The value set by the **ospfv3 cost** or **ipv6 ospf cost** command overrides the cost resulting from the **auto-cost** command.

Examples

The following example sets the auto-cost reference bandwidth to 1000 Mbps:

```
router ospfv3 1
 auto-cost reference-bandwidth 1000
```

Related Commands

Command	Description
ipv6 ospf cost	Explicitly specifies the cost of sending an IPv6 packet on an interface.
ospfv3 cost	Explicitly specifies the cost of sending a packet on an OSPFv3 interface.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

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.

bandwidth (interface)

To set the inherited and received bandwidth values for an interface, use the **bandwidth** command in interface configuration mode. To restore the default values, use the **no** form of this command.

bandwidth {*kbps* | **inherit** [*kbps*] | **receive** [*kbps*]}

no bandwidth {*kbps* | **inherit** [*kbps*] | **receive** [*kbps*]}

Syntax Description

kbps	Intended bandwidth, in kilobits per second. Valid values are 1 to 10000000. For a full bandwidth DS3 line, enter the value 44736.
inherit	(Optional) Inherited bandwidth. Specifies how a subinterface inherits the bandwidth of its main interface.
receive	(Optional) Receiver bandwidth. Entering this option enables asymmetric transmit/receive operations so that the transmitted (**inherit** [*kbps*]) and received bandwidth are different.

Command Default

Default bandwidth values are set during startup. The bandwidth values can be displayed using the **show interfaces** or **show ipv6 interface** command. If the receive keyword is not used, by default, the transmit and receive bandwidths are the same.

Command Modes

Interface configuration (config-if)
Virtual network interface (config-if-vnet)

Command History

Release	Modification
10.0	This command was introduced.
12.2T	The **inherit** keyword was added.
12.4(6)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.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

Bandwidth Information

The **bandwidth** command sets an informational parameter to communicate only the current bandwidth to the higher-level protocols; you cannot adjust the actual bandwidth of an interface using this command.

Note This is a routing parameter only. It does not affect the physical interface.

Changing Bandwidth

For some media, such as Ethernet, the bandwidth is fixed; for other media, such as serial lines, you can change the actual bandwidth by adjusting hardware. For both classes of media, you can use the **bandwidth** command to communicate the current bandwidth to the higher-level protocols.

Bandwidth Inheritance

Before the introduction of the **bandwidth inherit** command option, when the bandwidth value was changed on the main interface, existing subinterfaces did not inherit the bandwidth value from the main interface. If the subinterface was created before the bandwidth was changed on the main interface, then the subinterface would receive the default bandwidth of the main interface, not the configured bandwidth. Additionally, if the router was subsequently reloaded, the bandwidth of the subinterface would then change to the bandwidth configured on the main interface.

The **bandwidth inherit** command controls how a subinterface inherits the bandwidth of its main interface. This functionality eliminates the inconsistencies related to whether the router has been reloaded and what the order was in entering the commands.

The **no bandwidth inherit** command enables all subinterfaces to inherit the default bandwidth of the main interface, regardless of the configured bandwidth. If a bandwidth is not configured on a subinterface, and you use the **bandwidth inherit** command, all subinterfaces will inherit the current bandwidth of the main interface. If you configure a new bandwidth on the main interface, all subinterfaces will use this new value.

If you do not configure a bandwidth on the subinterface and you configure the **bandwidth inherit** *kbps* command on the main interface, the subinterfaces will inherit the specified bandwidth.

In all cases, if an interface has an explicit bandwidth setting configured, then that interface will use that setting, regardless of whether the bandwidth inheritance setting is in effect.

Bandwidth Receipt

Some interfaces (such as ADSL, V.35, RS-449, and HSSI serial interfaces) can operate with different transmit and receive bandwidths. The **bandwidth receive** command permits this type of asymmetric operation. For example, for ADSL, the lower layer detects the two bandwidth values and configures the IDB accordingly. Other interface drivers, particularly serial interface cards on low- and midrange-platforms) can operate in this asymmetric bandwidth mode but cannot measure their clock rates. In these cases, administrative configuration is necessary for asymmetric operations.

Examples

The following example shows how to set the full bandwidth for DS3 transmissions:

```
Router(config)# interface serial 0
Router(config-if)# bandwidth 44736
```

The following example shows how to set the receive bandwidth:

```
Router(config)# interface serial 0
Router(config-if)# bandwidth receive 1000
```

Related Commands

Command	Description
show interfaces	Displays statistics for all interfaces configured on the router.
show ipv6 interface	Displays statistics for all interfaces configured on the IPv6 router.

bfd

To set the baseline Bidirectional Forwarding Detection (BFD) session parameters on an interface, use the **bfd** command in interface configuration mode. To remove the baseline BFD session parameters, use the **no** form of this command.

bfd interval *milliseconds* **min_rx** *milliseconds* **multiplier** *multiplier-value*

no bfd interval *milliseconds* **min_rx** *milliseconds* **multiplier** *multiplier-value*

Syntax Description

interval *milliseconds*	Specifies the rate at which BFD control packets will be sent to BFD peers. The configurable time period for the *milliseconds* argument is from 50 to 999 milliseconds (ms).
min_rx *milliseconds*	Specifies the rate at which BFD control packets will be expected to be received from BFD peers. The configurable time period for the *milliseconds* argument is from 50 to 999 ms.
multiplier *multiplier-value*	Specifies the number of consecutive BFD control packets that must be missed from a BFD peer before BFD declares that the peer is unavailable and the Layer 3 BFD peer is informed of the failure. The configurable value range for the *multiplier-value* argument is from 3 to 50.

Command Default

No baseline BFD session parameters are set.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)SXE	This command was introduced.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S.
12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	This command was implemented on Cisco ASR 1000 Series Aggregation Services Routers.
12.2(33)SRE	This command was modified. Support for IPv6 was added.
15.0(1)M	This command was modified. Support was removed from ATM and inverse multiplexing over ATM (IMA) interfaces.
15.1(2)T	This command was modified. Support for IPv6 was added to Cisco IOS Release 15.1(2)T.

Usage Guidelines

The **bfd** command can be configured on the following interfaces:

- ATM
- Dot1Q VLAN subinterfaces (with an IP address on the Dot1Q subinterface)
- Ethernet
- Frame Relay
- IMA
- PoS
- Serial

Other interface types are not supported by BFD.

Note The **bfd interval** command is not supported on ATM and IMA interfaces in Cisco IOS Release 15.0(1)M and later releases.

Examples

The following example shows the BFD session parameters set for Fast Ethernet interface 3/0:

```
Router> enable
Router# configure terminal
Router(config)# interface fastethernet 3/0
Router(config-if)# bfd interval 50 min_rx 50 multiplier 3
Router(config-if)# end
```

Related Commands

Command	Description
bfd all-interfaces	Enables BFD for all interfaces for a BFD peer.
bfd interface	Enables BFD on a per-interface basis for a BFD peer.
clear bfd	Clears BFD session parameters.
ip ospf bfd	Enables BFD on a specific interface configured for OSPF.

bfd all-interfaces

To enable Bidirectional Forwarding Detection (BFD) for all interfaces participating in the routing process, use the **bfd all-interfaces** command in router configuration or address-family interface configuration mode. To disable BFD for all neighbors on a single interface, use the **no** form of this command.

bfd all-interfaces

no bfd all-interfaces

Syntax Description

This command has no arguments or keywords.

Command Default

BFD is disabled on the interfaces participating in the routing process.

Command Modes

Router configuration (config-router) and address-family interface configuration (config-router-af)

Command History

Release	Modification
12.2(18)SXE	This command was introduced.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S.
12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS Release 2.1 XE	This command was integrated into Cisco IOS Release 2.1 XE and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.
12.2(33)SRE	This command was modified. Support for IPv6 was added.
15.0(1)M	This command was modified. The **bfd all-interfaces** command in named router configuration mode was replaced by the **bfd** command in address-family interface mode.
15.1(2)T	This command was modified. Support for IPv6 was added.
Cisco IOS XE Release 3.3	This command was modified. Support for the Routing Information Protocol was added.

Usage Guidelines

There are two methods to configure routing protocols to use BFD for failure detection. To enable BFD for all interfaces, enter the **bfd all-interfaces** command in router configuration mode. In Cisco IOS Release 12.4(24)T, Cisco IOS 12.2(33)SRA and earlier releases, the **bfd all-interfaces** command works in router configuration mode and address-family interface mode.

In Cisco IOS Release 15.0(1)M and later releases, the **bfd all-interfaces** command in named router configuration mode is replaced by the **bfd** command in address-family interface configuration mode. Use the **bfd** command in address-family interface configuration mode to achieve the same functionality as that of the **bfd all interfaces** command in router configuration mode.

Examples

The following example shows how to enable BFD for all Enhanced Interior Gateway Routing Protocol (EIGRP) neighbors:

```
Router> enable
Router# configure terminal
Router(config)# router eigrp 123
Router(config-router)# bfd all-interfaces
Router(config-router)# end
```

The following example shows how to enable BFD for all Intermediate System-to-Intermediate System (IS-IS) neighbors:

```
Router> enable
Router# configure terminal
Router(config)# router isis tag1
Router(config-router)# bfd all-interfaces
Router(config-router)# end
```

The following example shows how to enable BFD for all Open Shortest Path First (OSPF) neighbors:

```
Router> enable
Router# configure terminal
Router(config)# router ospf 123
Router(config-router)# bfd all-interfaces
Router(config-router)# end
```

The following example shows how to enable BFD for all EIGRP neighbors, using the **bfd** command in address-family interface configuration mode:

```
Router> enable
Router# configure terminal
Router(config)# router eigrp my_eigrp
Router(config-router)# address-family ipv4 autonomous-system 100
Router(config-router-af)# af-interface FastEthernet 0/0
Router(config-router-af-interface)# bfd
```

The following example shows how to enable BFD for all Routing Information Protocol (RIP) neighbors:

```
Router> enable
Router# configure terminal
Router(config)# router rip
Router(config-router)# bfd all-interfaces
Router(config-router)# end
```

Related Commands

Command	Description
bfd	Sets the baseline BFD session parameters on an interface.

bfd all-interfaces (OSPFv3)

To enable Bidirectional Forwarding Detection (BFD) for an Open Shortest Path First version 3 (OSPFv3) routing process, use the **bfd all-interfaces** command in OSPFv3 router configuration mode. To disable BFD for the OSPFv3 routing process, use the **no** form of this command.

bfd all-interfaces

no bfd all-interfaces

Syntax Description

This command has no arguments or keywords.

Command Default

BFD is disabled on the interfaces participating in the routing process.

Command Modes

OSPFv3 router configuration mode (config-router)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

Use the **bfd all-interfaces** command in OSPFv3 router configuration mode to enable BFD for all OSPFv3 interfaces.

Examples

The following example shows how to enable BFD for all Open Shortest Path First (OSPF) neighbors:

```
Router(config)# router ospfv3 123
Router(config-router)# bfd all-interfaces
Router(config-router)# end
```

Related Commands

Command	Description
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

bgp additional-paths install

To enable BGP to calculate a backup path for a given address family and to install it into the Routing Information Base (RIB) and Cisco Express Forwarding, use the **bgp additional-paths install** command in address family configuration or router configuration mode. To remove the backup paths, use the **no** form of this command.

bgp additional-paths install

no bgp additional-paths install

Syntax Description

This command has no arguments or keywords.

Command Default

A backup path is not created.

Command Modes

Address family configuration (config-router-af)
Router configuration (config-router)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.
Cisco IOS XE Release 3.3S	Support for IPv6 address family configuration mode was added.
15.1(2)S	Support for IPv6 address family configuration mode was added.

Usage Guidelines

You can issue the **bgp additional-paths install** command in different modes, each of which protects VRFs in its own way:

- VPNv4 address family configuration mode protects all VRFs.
- IPv4 address family configuration mode protects only IPv4 VRFs.
- IPv6 address family configuration mode protects only IPv6 VRFs.
- Router configuration mode protects VRFs in the global routing table.

Examples

The following example shows how to calculate a backup path and install it into the RIB and Cisco Express Forwarding:

```
Router(config-router-af)# bgp additional-paths install
```

Related Commands

Command	Description
address-family ipv6	Enters address family configuration mode for configuring routing sessions such as BGP that use standard IPv6 address prefixes.
bgp advertise-best-external	Enables BGP to use an external route as the backup path after a link or node failure.

bgp advertise-best-external

To enable BGP to calculate an external route as the best backup path for a given address family and to install it into the Routing Information base (RIB) and Cisco Express Forwarding, and to advertise the best external path to its neighbors, use the **bgp advertise-best-external** command in address family or router configuration mode. To remove the external backup path, use the **no** form of this command.

bgp advertise-best-external

no bgp advertise-best-external

Syntax Description

This command has no arguments or keywords.

Command Default

An external backup path is not created.

Command Modes

Router configuration (config-router)
Address family configuration (config-router-af)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
Cisco IOS XE Release 3.3S	Support for IPv6 address family configuration mode was added.
15.1(2)S	Support for IPv6 address family configuration mode was added.

Usage Guidelines

When you configure the Best External feature with the **bgp advertise-best-external** command, you need not enable the Prefix Independent Convergence (PIC) feature with the **bgp additional-paths install** command. The Best External feature automatically installs a backup path. If you try to configure the PIC feature after configuring the Best External feature, you receive an error. This behavior applies to both BGP and MPLS.

When you configure the MPLS VPN: Best External feature with the **bgp advertise-best-external** command, it will override the functionality of the MPLS VPN—BGP Local Convergence feature. You need not remove the **protection local-prefixes** command from the configuration.

You can issue the **bgp advertise-best-external** command in different modes, each of which protects VRFs in its own way:

- VPNv4 address-family configuration mode protects all VRFs.
- IPv4 address-family configuration mode protects only IPv4 VRFs.
- IPv6 address family configuration mode protects only IPv6 VRFs.
- Router configuration mode protects VRFs in the global routing table.

Examples

The following example calculates an external backup path and installs it into the RIB and Cisco Express Forwarding:

```
Router(config-router-af)# bgp advertise-best-external
```

Related Commands

Command	Description
address-family ipv6	Enters address family configuration mode for configuring routing sessions such as BGP that use standard IPv6 address prefixes.
bgp additional-paths install	Enables BGP to use an additional path as the backup path.
protection local-prefixes	Enables PE–CE link protection by preserving the local label.

bgp default ipv6-nexthop

To set the IPv6 unicast next-hop format as the default for Border Gateway Protocol (BGP) IPv6 updates, use the **bgp default ipv6-nexthop** command in router configuration mode. To disable the default IPv6 unicast next-hop format as the default, use the **no** form of this command.

bgp default ipv6-nexthop

no bgp default ipv6-nexthop

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled by default and is not shown in the running configuration.

Command Modes

Router configuration

Command History

Release	Modification
12.0(32)SY9	This command was introduced.

Usage Guidelines

The **bgp default ipv6-nexthop** command enables BGP to choose the IPv6 next hop automatically for IPv6 address family prefixes.

Use the **no bgp default ipv6-nexthop** command to disable automatic next-hop selection in the following situations when IPv6 next-hop selection is configured to propagate over IPv4 sessions:

- If a route map is applied, then use the next hop given in the route map.
- If a route map is not configured, do one of the following:
  - If the router has directly connected peering configured, pick up a IPv6 address (both global and link-local IPv6 addresses)
  - If loopback peering is configured, pick up a IPv6 address from the loopback interface (both global and link-local IPv6 addresses)
  - The router configuration falls back to the default behavior of a IPv4-mapped IPv6 address.

Examples

The following example disables the unicast next-hop format for router process 50000:

```
Router(config)# router bgp 50000
Router(config-router)# no bgp default ipv6-nexthop
```

bgp graceful-restart

To enable the Border Gateway Protocol (BGP) graceful restart capability globally for all BGP neighbors, use the **bgp graceful-restart** command in address family or in router configuration mode. To disable the BGP graceful restart capability globally for all BGP neighbors, use the **no** form of this command.

bgp graceful-restart [**restart-time** *seconds* | **stalepath-time** *seconds*] [**all**]

no bgp graceful-restart

Syntax Description

restart-time *seconds*	(Optional) Sets the maximum time period that the local router will wait for a graceful-restart-capable neighbor to return to normal operation after a restart event occurs. The default value for this argument is 120 seconds. The configurable range of values is from 1 to 3600 seconds.
stalepath-time *seconds*	(Optional) Sets the maximum time period that the local router will hold stale paths for a restarting peer. All stale paths are deleted after this timer expires. The default value for this argument is 360 seconds. The configurable range of values is from 1 to 3600 seconds
all	(Optional) Enables BGP graceful restart capability for all address family modes.

Command Default

The following default values are used when this command is entered without any keywords or arguments:

restart-time: 120 seconds
stalepath-time: 360 seconds

Note Changing the restart and stalepath timer values is not required to enable the BGP graceful restart capability. The default values are optimal for most network deployments, and these values should be adjusted only by an experienced network operator.

Command Modes

Address-family configuration (config-router-af)
Router configuration (config-router)

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(28)SB	Support for this command was added 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.

Release	Modification
Cisco IOS XE Release 2.1	Support for IPv6 was added. The optional **all** keyword was added.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

The **bgp graceful-restart** command is used to enable or disable the graceful restart capability globally for all BGP neighbors in a BGP network. The graceful restart capability is negotiated between nonstop forwarding (NSF)-capable and NSF-aware peers in OPEN messages during session establishment. If the graceful restart capability is enabled after a BGP session has been established, the session will need to be restarted with a soft or hard reset.

The graceful restart capability is supported by NSF-capable and NSF-aware routers. A router that is NSF-capable can perform a stateful switchover (SSO) operation (graceful restart) and can assist restarting peers by holding routing table information during the SSO operation. A router that is NSF-aware functions like a router that is NSF-capable but cannot perform an SSO operation.

The BGP graceful restart capability is enabled by default when a supporting version of Cisco IOS software is installed. The default timer values for this feature are optimal for most network deployments. We recommend that they are adjusted only by experienced network operators. When adjusting the timer values, the restart timer should not be set to a value greater than the hold time that is carried in the OPEN message. If consecutive restart operations occur, routes (from a restarting router) that were previously marked as stale will be deleted.

Note Changing the restart and stalepath timer values is not required to enable the BGP graceful restart capability. The default values are optimal for most network deployments, and these values should be adjusted only by an experienced network operator.

Examples

In the following example, the BGP graceful restart capability is enabled:

```
Router# configure terminal
Router(config)# router bgp 65000
Router(config-router)# bgp graceful-restart
```

In the following example, the restart timer is set to 130 seconds:

```
Router# configure terminal
Router(config)# router bgp 65000
Router(config-router)# bgp graceful-restart restart-time 130
```

In the following example, the stalepath timer is set to 350 seconds:

```
Router# configure terminal
Router(config)# router bgp 65000
Router(config-router)# bgp graceful-restart stalepath-time 350
```

Related Commands

Command	Description
show ip bgp	Displays entries in the BGP routing table.
show ip bgp neighbors	Displays information about the TCP and BGP connections to neighbors.

bgp log-neighbor-changes

To enable logging of BGP neighbor resets, use the **bgp log-neighbor-changes** command in router configuration mode. To disable the logging of changes in BGP neighbor adjacencies, use the **no** form of this command.

bgp log-neighbor-changes

no bgp log-neighbor-changes

Syntax Description

This command has no arguments or keywords.

Command Default

Logging of BGP neighbor resets is not enabled.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
11.1CC	This command was introduced.
12.0	This command was integrated into Cisco IOS release 12.0.
12.0(7)T	Address family configuration mode support was added.
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.

Usage Guidelines

The **bgp log-neighbor-changes** command enables logging of BGP neighbor status changes (up or down) and resets for troubleshooting network connectivity problems and measuring network stability. Unexpected neighbor resets might indicate high error rates or high packet loss in the network and should be investigated.

Using the **bgp log-neighbor-changes** command to enable status change message logging does not cause a substantial performance impact, unlike, for example, enabling per BGP update debugging. If the UNIX syslog facility is enabled, messages are sent to the UNIX host running the syslog daemon so that the messages can be stored and archived. If the UNIX syslog facility is not enabled, the status change messages are retained in the internal buffer of the router, and are not stored to disk. You can set the size of this buffer, which is dependent upon the available RAM, using the **logging buffered** command.

The neighbor status change messages are not tracked if the **bgp log-neighbor-changes** command is not enabled, except for the reset reason, which is always available as output of the **show ip bgp neighbors** and **show bgp ipv6 neighbors** commands.

The **eigrp log-neighbor-changes** command enables logging of Enhanced Interior Gateway Routing Protocol (EIGRP) neighbor adjacencies, but messages for BGP neighbors are logged only if they are specifically enabled with the **bgp log-neighbor-changes** command.

Use the **show logging** command to display the log for the BGP neighbor changes.

Examples

The following example logs neighbor changes for BGP in router configuration mode:

```
Router(config)# bgp router 40000
Router(config-router)# bgp log-neighbor-changes
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
eigrp log-neighbor-changes	Enables the logging of neighbor adjacency changes to monitor the stability of the routing system and to help detect problems.
logging buffered	Logs messages to an internal buffer.
show ip bgp ipv4	Displays information about the TCP and BGP connections to neighbors.
show ip bgp neighbors	Displays information about BGP neighbors.
show logging	Displays the state of logging (syslog).

bgp recursion host

To enable the recursive-via-host flag for IP Version 4 (IPv4), Virtual Private Network (VPN) Version 4 (VPNv4), Virtual Routing and Forwarding (VRF) address families, and IPv6 address families, use the **bgp recursion host** command in address family configuration or router configuration mode. To disable the recursive-via-host flag, use the **no** form of this command.

bgp recursion host

no bgp recursion host

Syntax Description

This command has no arguments or keywords.

Command Default

For an internal Border Gateway Protocol (iBGP) IPv4 address family, irrespective of whether Prefix Independent Convergence (PIC) is enabled, the recursive-via-host flag in Cisco Express Forwarding is not set.

For the VPNv4 and IPv4 VRF address families, the recursive-via-host flag is set and the **bgp recursion host** command is automatically restored when PIC is enabled under the following conditions:

- The **bgp additional-paths install** command is enabled.
- The **bgp advertise-best-external** command is enabled.

Command Modes

Address family configuration (config-router-af)
Router configuration (config-router)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.
Cisco IOS XE Release 3.3S	Support for IPv6 address family configuration mode was added.
15.1(2)S	Support for IPv6 address family configuration mode was added.

Usage Guidelines

The **bgp recursion host** command is used to help Cisco Express Forwarding during traffic blackholing when a node failure occurs.

For link protection, BGP automatically restricts the recursion for the next hop resolution of connected routes. These routes are provided by the route reflector, which receives the prefix from another provider edge (PE) router that needs the customer edge (CE) router to be protected.

For node protection, BGP automatically restricts the recursion for the next hop resolution of host routes. These routes are provided by the route reflector, which receives the prefix from the host PE router. If a PE router or Autonomous System Boundary Router (ASBR) fails, for the **bgp recursion host** command to work, the PE routers must satisfy the following options:

- The host prefix must be used on the PE loopback interfaces.
- The next-hop-self must be configured on iBGP sessions.
- The **recursive via host prefix** command must be configured.

To enable Cisco Express Forwarding to use strict recursion rules for an IPv4 address family, you must configure the **bgp recursion host** command that enables the **recursive-via-host** flag when PIC is enabled.

The recursive-via-connected flag is set for directly connected peers only. For example, if the **bgp additional-paths install** command is configured in IPv4 and IPv4 VRF address family configuration modes, the running configuration shows the following details:

```
address-family ipv4
bgp additional-paths-install
no bgp recursion host
!
address-family ipv4 vrf red
bgp additional-paths-install
bgp recursion host
```

In the case of an External Border Gateway Protocol (eBGP) directly connected peers route exchange, the recursion is disabled for the connected routes. The recursive-via-connected flag is automatically set in the RIB and Cisco Express Forwarding for the routes from the eBGP single-hop peers.

For all the VPNs, irrespective of whether PIC is enabled, when the **bgp recursion host** command is configured in VPNv4 and IPv4 address family configuration modes, the normal recursion rules are disabled and only recursion via host-specific routes are allowed for primary, backup, and multipaths under those address families. To enable the normal recursion rules, configure the **no bgp recursion host** command in VPNv4 and IPv4 address family configuration modes.

Examples

The following example shows the configuration of the **bgp advertise-best-external** and **bgp recursion host** commands:

```
Router> enable
Router# configure terminal
Router(config)# router ospf 10
Router(config-router)# log-adjacency-changes
Router(config-router)# redistribute connected subnets
Router(config-router)# network 192.168.0.0 0.0.255.255 area 0
Router(config-router)# router bgp 64500
Router(config-router)# no synchronization
Router(config-router)# bgp log-neighbor-changes
Router(config-router)# neighbor 10.5.5.5 remote-as 64500
Router(config-router)# neighbor 10.5.5.5 update-source Loopback0
Router(config-router)# neighbor 10.6.6.6 remote-as 64500
Router(config-router)# neighbor 10.6.6.6 update-source Loopback0
Router(config-router)# no auto-summary
Router(config-router)# address-family vpnv4
Router(config-router-af)# neighbor 10.5.5.5 activate
Router(config-router-af)# neighbor 10.5.5.5 send-community extended
Router(config-router-af)# neighbor 10.6.6.6 activate
Router(config-router-af)# neighbor 10.6.6.6 send-community extended
Router(config-router-af)# exit-address-family
Router(config-router)# address-family ipv4 vrf test1
```

```
Router(config-router-af)# no synchronization
Router(config-router-af)# bgp advertise-best-external
Router(config-router-af)# bgp recursion host
Router(config-router-af)# neighbor 192.168.9.2 remote-as 64511
Router(config-router-af)# neighbor 192.168.9.2 fall-over bfd
Router(config-router-af)# neighbor 192.168.9.2 activate
Router(config-router-af)# neighbor 192.168.9.2 as-override
Router(config-router-af)# neighbor 192.168.9.2 route-map LOCAL_PREF in
Router(config-router-af)# exit-address-family
```

The following example shows the configuration of the **bgp additional-paths install** and **bgp recursion host** commands:

```
Router> enable
Router# configure terminal
Router(config)# router ospf 10
Router(config-router)# log-adjacency-changes
Router(config-router)# redistribute connected subnets
Router(config-router)# network 192.168.0.0 0.0.255.255 area 0
Router(config-router)# router bgp 64500
Router(config-router)# no synchronization
Router(config-router)# bgp log-neighbor-changes
Router(config-router)# neighbor 10.5.5.5 remote-as 64500
Router(config-router)# neighbor 10.5.5.5 update-source Loopback0
Router(config-router)# neighbor 10.6.6.6 remote-as 64500
Router(config-router)# neighbor 10.6.6.6 update-source Loopback0
Router(config-router)# no auto-summary
Router(config-router)# address-family vpnv4
Router(config-router-af)# neighbor 10.5.5.5 activate
Router(config-router-af)# neighbor 10.5.5.5 send-community extended
Router(config-router-af)# neighbor 10.6.6.6 activate
Router(config-router-af)# neighbor 10.6.6.6 send-community extended
Router(config-router-af)# exit-address-family
Router(config-router)# address-family ipv4 vrf test1
Router(config-router-af)# no synchronization
Router(config-router-af)# bgp additional-paths install
Router(config-router-af)# bgp recursion host
Router(config-router-af)# neighbor 192.168.9.2 remote-as 64511
Router(config-router-af)# neighbor 192.168.9.2 fall-over bfd
Router(config-router-af)# neighbor 192.168.9.2 activate
Router(config-router-af)# neighbor 192.168.9.2 as-override
Router(config-router-af)# neighbor 192.168.9.2 route-map LOCAL_PREF in
Router(config-router-af)# exit-address-family
```

The following example shows the best external routes and the BGP recursion flags enabled:

```
Router# show ip bgp vpnv4 vrf test1 192.168.13.1

BGP routing table entry for 400:1:192.168.13.0/24, version 4
Paths: (2 available, best #2, table test1)
  Advertise-best-external
  Advertised to update-groups:
     1
  64511, imported path from 300:1:192.168.13.0/24
    10.7.7.7 (metric 20) from 10.5.5.5 (10.5.5.5)
      Origin IGP, metric 0, localpref 50, valid, internal, backup/repair
      Extended Community: RT:100:1 RT:200:1 RT:300:1 RT:400:1
      Originator: 10.7.7.7, Cluster list: 10.5.5.5 , recursive-via-host
      mpls labels in/out 25/17
  64511
    10.8.8.8 from 10.8.8.8 (192.168.13.1)
      Origin IGP, metric 0, localpref 100, valid, external, best
      Extended Community: RT:100:1 RT:200:1 RT:300:1 RT:400:1 , recursive-via-connected
      mpls labels in/out 25/nolabel
```

The following example shows the additional paths and the BGP recursion flags enabled:

```
Router# show ip bgp vpnv4 vrf test1 192.168.13.1

BGP routing table entry for 400:1:192.168.13.0/24, version 25
Paths: (2 available, best #2, table test1)
  Additional-path
  Advertised to update-groups:
     1
  64511, imported path from 300:1:192.168.13.0/24
    10.7.7.7 (metric 20) from 10.5.5.5 (10.5.5.5)
      Origin IGP, metric 0, localpref 50, valid, internal, backup/repair
      Extended Community: RT:100:1 RT:200:1 RT:300:1 RT:400:1
      Originator: 10.7.7.7, Cluster list: 10.5.5.5 , recursive-via-host
      mpls labels in/out 25/17
  64511
    10.8.8.8 from 10.8.8.8 (192.168.13.1)
      Origin IGP, metric 0, localpref 100, valid, external, best
      Extended Community: RT:100:1 RT:200:1 RT:300:1 RT:400:1 , recursive-via-connected
      mpls labels in/out 25/nolabel
```

Table 7 describes the significant fields shown in the display.

Table 7 show ip bgp vpnv4 vrf network-address Field Descriptions

Field	Description
BGP routing table entry for ... version	Internal version number of the table. This number is incremented whenever the table changes.
Paths	Number of autonomous system paths to the specified network. If multiple paths exist, one of the multipaths is designated the best path.
Advertised to update-groups	IP address of the BGP peers to which the specified route is advertised.
10.7.7.7 (metric 20) from 10.5.5.5 (10.5.5.5)	Indicates the next hop address and the address of the gateway that sent the update.
Origin	Indicates the origin of the entry. It can be one of the following values: • IGP—Entry originated from Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • incomplete—Entry originated from other than an IGP or Exterior Gateway Protocol (EGP) and was advertised with the **redistribute** router configuration command. • EGP—Entry originated from an EGP.
metric	The value of the interautonomous system metric.
localpref	Local preference value as set with the **set local-preference route-map** configuration command. The default value is 50.
valid	Indicates that the route is usable and has a valid set of attributes.
internal/external	The field is *internal* if the path is learned via iBGP. The field is *external* if the path is learned via eBGP.
best	If multiple paths exist, one of the multipaths is designated the best path and this path is advertised to neighbors.

Table 7 show ip bgp vpnv4 vrf network-address Field Descriptions (continued)

Field	Description
Extended Community	Route Target value associated with the specified route.
Originator	The router ID of the router from which the route originated when route reflector is used.
Cluster list	The router ID of all the route reflectors that the specified route has passed through.

Related Commands

Command	Description
address-family ipv6	Enters address family configuration mode for configuring routing sessions such as BGP that use standard IPv6 address prefixes.
bgp advertise-best-external	Enables BGP to use an external route as the backup path after a link or node failure.
bgp additional-paths install	Enables BGP to use an additional path as the backup path.

bgp router-id

To configure a fixed router ID for the local Border Gateway Protocol (BGP) routing process, use the **bgp router-id** command in router or address family configuration mode. To remove the fixed router ID from the running configuration file and restore the default router ID selection, use the **no** form of this command.

Router Configuration

bgp router-id {*ip-address* | **vrf auto-assign**}

no bgp router-id [**vrf auto-assign**]

Address Family Configuration

bgp router-id {*ip-address* | **auto-assign**}

no bgp router-id

Syntax Description

ip-address	Router identifier in the form of an IP address.
vrf	Configures a router identifier for a Virtual Routing and Forwarding (VRF) instance.
auto-assign	Automatically assigns a router identifier for each VRF.

Command Default

The following behavior determines local router ID selection when this command is not enabled:

- If a loopback interface is configured, the router ID is set to the IP address of the loopback interface. If multiple loopback interfaces are configured, the router ID is set to the IP address of the loopback interface with the highest IP address.
- If no loopback interface is configured, the router ID is set to the highest IP address on a physical interface.

Command Modes

Address family configuration (config-router-af)
Router configuration (config-router)

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	The **vrf** and **auto-assign** keywords were added, and this command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command, including the **vrf** and **auto-assign** keywords, was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command, including the **vrf** and **auto-assign** keywords, was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	The **vrf** and **auto-assign** keywords were added.

Usage Guidelines

The **bgp router-id** command is used to configure a fixed router ID for the local BGP routing process. The router ID is entered in IP address format. Any valid IP address can be used, even an address that is not locally configured on the router. If you use an IP address from a local interface, we recommend that you use the address of a loopback interface rather than the address of a physical interface. (A loopback interface is more effective than a fixed interface as an identifier because there is no physical link to go down.) Peering sessions are automatically reset when the router ID is changed.

In Cisco IOS Release 12.2(33)SRA, 12.2(31)SB2, 12.2(33)SXH, 12.4(20)T, and later releases, the Per-VRF Assignment of BGP Router ID feature introduced VRF-to-VRF peering in BGP on the same router. BGP is designed to refuse a session with itself because of the router ID check. The per-VRF assignment feature allows a separate router ID per VRF. The router ID can be manually configured for each VRF or automatically assigned either for each VRF or globally under address family configuration mode.

Examples

The following example shows how to configure the local router with a fixed BGP router ID of 192.168.254.254:

```
router bgp 50000
 bgp router-id 192.168.254.254
```

The following example shows how to configure a BGP router ID for the VRF named VRF1. This configuration is done under address family IPv4 VRF configuration mode.

```
router bgp 45000
 address-family ipv4 vrf VRF1
  bgp router-id 10.1.1.99
```

The following example shows how to configure an automatically assigned VRF BGP router ID for all VRFs. This configuration is done under BGP router configuration mode.

```
router bgp 45000
 bgp router-id vrf auto-assign
```

The following example shows how to configure an automatically assigned VRF BGP router ID for a single VRF. This configuration is done under address family IPv4 VRF configuration mode.

```
router bgp 45000
 address-family ipv4 vrf VRF2
  bgp router-id auto-assign
```

Related Commands

Command	Description
show ip bgp	Displays entries in the BGP routing table.
show ip bgp vpnv4	Displays VPNv4 address information from the BGP routing table.

bind

To bind the source address for signaling and media packets to the IPv4 or IPv6 address of a specific interface, use the **bind** command in SIP configuration mode. To disable binding, use the **no** form of this command.

bind {**control** | **media** | **all**} **source-interface** *interface-id* [**ipv4-address** *ipv4-address* | **ipv6-address** *ipv6-address*]

no bind

Syntax Description

control	Binds Session Initiation Protocol (SIP) signaling packets.
media	Binds only media packets.
all	Binds SIP signaling and media packets. The source address (the address that shows where the SIP request came from) of the signaling and media packets is set to the IPv4 or IPv6 address of the specified interface.
source-interface	Specifies an interface as the source address of SIP packets.
interface-id	Specifies one of the following interfaces: • **Async**: ATM interface • **BVI**: Bridge-Group Virtual Interface • **CTunnel**: CTunnel interface • **Dialer**: Dialer interface • **Ethernet**: IEEE 802.3 • **FastEthernet**: Fast Ethernet • **Lex**: Lex interface • **Loopback**: Loopback interface • **Multilink**: Multilink-group interface • **Null**: Null interface • **Serial**: Serial interface (Frame Relay) • **Tunnel**: Tunnel interface • **Vif**: PGM Multicast Host interface • **Virtual-Template**: Virtual template interface • **Virtual-TokenRing**: Virtual token ring
ipv4-address *ipv4-address*	(Optional) Configures the IPv4 address. Several IPv4 addresses can be configured under one interface.
ipv6-address *ipv6-address*	(Optional) Configures the IPv6 address under an IPv4 interface. Several IPv6 addresses can be configured under one IPv4 interface.

Command Default

Binding is disabled.

Command Modes

SIP configuration (conf-serv-sip)

Command History

Release	Modification
12.2(2)XB	This command was introduced on the Cisco 2600 series, Cisco 3600 series, Cisco 7200 series, Cisco AS5300, Cisco AS5350, and Cisco AS5400.
12.2(2)XB2	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. This command does not support the Cisco AS5300, Cisco AS5350, Cisco AS5850, and Cisco AS5400 in this release.
12.3(4)T	The **media** keyword was added.
12.4(22)T	Support for IPv6 was added.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5

Usage Guidelines

Async, Ethernet, FastEthernet, Loopback, and Serial (including Frame Relay) are interfaces within the SIP application.

If the **bind** command is not enabled, the IPv4 layer still provides the best local address.

Examples

The following example sets up binding on a SIP network:

```
Router(config)# voice serv voip
Router(config-voi-serv)# sip
Router(config-serv-sip)# bind control source-interface FastEthernet 0
```

Related Commands

Command	Description
sip	Enters SIP configuration mode from voice service VoIP configuration mode.

binding

To configure binding options for the Mobile IPv6 home agent feature, use the **binding** command in home agent configuration mode. To restore parameters to default values, use the **no** form of this command.

binding [**access** *access-list-name* | *auth-option* | *seconds* | *maximum* | *refresh*]

no binding [**access** *access-list-name* | *auth-option* | *seconds* | *maximum* | *refresh*]

Syntax Description

access	(Optional) Specifies an access list to limit response.
access-list-name	(Optional) Access control list used to configure a binding update filter. When an access control list is configured, all Dynamic Home Agent Address Discovery (DHAAD) requests and binding updates are filtered by the home address and destination address.
auth-option	(Optional) Valid authentication option, which authenticates the binding update and binding acknowledgment messages based on the shared-key-based security association between the mobile node and the home agent.
seconds	(Optional) Permissible maximum binding lifetime, in number of seconds. The lifetime granted in the binding acknowledgment (binding ack) parameter is always the smallest of the requested lifetime, subnet lifetime, and configured permissible lifetime parameters.
maximum	(Optional) Maximum number of binding cache entries. If the value is set to 0, no new binding requests are accepted. Existing bindings are allowed to expire gracefully.
refresh	(Optional) Suggested binding refresh interval, in number of seconds. If the registration lifetime is greater than the configured binding refresh interval, this value is returned to the mobile node in the binding refresh advice option in the binding ack sent by the home agent.

Command Default

No access list is used to configure a binding update filter.
The default value for the *seconds* argument is 262140, which is the maximum permissible binding time.
The default value for the *maximum* argument is a number of entries limited by memory available on the router.
The default value of the *refresh* argument is 300 sec.

Command Modes

Home agent configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(11)T	The *auth-option* argument was added.
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.

Usage Guidelines

Before you enable the **ipv6 mobile home-agent** command on an interface, you should configure common parameters on the router using the **binding** command. This command does not enable home agent service on the interfaces.

If the configured number of home agent registrations is reached or exceeded, subsequent registrations will be refused with the error "Insufficient resources." No existing bindings will discarded until their lifetime has expired, even if the *maximum* argument is set to a value lower than the current number of such bindings.

The appropriate value for the *refresh* argument will depend on whether the router is operating any high-availability features. If it is not, and a failure would cause the bindings cache to be lost, set the *refresh* argument to a low value.

Examples

In the following example, the maximum number of binding cache entries is set to 15:

```
binding 15
```

Related Commands

Command	Description
ipv6 mobile home-agent (global configuration)	Enters home agent configuration mode.
ipv6 mobile home-agent (interface configuration)	Initializes and starts the Mobile IPv6 home agent on a specific interface.
show ipv6 mobile globals	Displays global Mobile IPv6 parameters.

bridge-group

To assign each network interface to a bridge group, use the **bridge-group** command in interface configuration mode. To remove the interface from the bridge group, use the **no** form of this command.

bridge-group *bridge-group*

no bridge-group *bridge-group*

Syntax Description

bridge-group	Number of the bridge group to which the interface belongs. It must be a number in the range from 1 to 255.

Defaults

No bridge group interface is assigned.

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 12.2(33)SRA.
15.1(2)T	Support for IPv6 was added.

Usage Guidelines

You can bridge on any interface, including any serial interface, regardless of encapsulation. Bridging can be configured between interfaces on different cards, although the performance is lower compared with interfaces on the same card. Also note that serial interfaces must be running with high-level data link control (HLDC), X.25, or Frame Relay encapsulation.

Note Several modifications to interfaces in bridge groups, including adding interfaces to bridge groups, will result in any Token Ring or FDDI interfaces in that bridge group being re initialized.

Examples

In the following example, Ethernet interface 0 is assigned to bridge group 1, and bridging is enabled on this interface:

```
interface ethernet 0
 bridge-group 1
```

Related Commands

Command	Description
bridge-group cbus-bridging	Enables autonomous bridging on a ciscoBus2 controller.
bridge-group circuit-group	Assigns each network interface to a bridge group.
bridge-group input-pattern-list	Associates an extended access list with a particular interface in a particular bridge group.
bridge-group output-pattern-list	Associates an extended access list with a particular interface.
bridge-group spanning-disabled	Disables the spanning tree on a given interface.

cache

To configure operational parameters for NetFlow accounting aggregation caches, use the **cache** command in NetFlow aggregation cache configuration mode. To disable the NetFlow aggregation cache operational parameters for NetFlow accounting, use the **no** form of this command.

cache {**entries** *number* | **timeout** {**active** *minutes* | **inactive** *seconds*}}

no cache {**entries | timeout** {**active | inactive**}}

Syntax Description

entries *number*	(Optional) The number of cached entries allowed in the aggregation cache. The range is from 1024 to 524288. The default is 4096. **Note** For the Cisco ASR 1000 Series Aggregation Services Router, the range is 1024 to 2000000 (2 million). The default is 4096.
timeout	(Optional) Configures aggregation cache time-outs.
active *minutes*	(Optional) The number of minutes that an active entry will stay in the aggregation cache before it is exported and removed. The range is from 1 to 60 minutes. The default is 30 minutes.
inactive *seconds*	(Optional) The number of seconds that an inactive entry will stay in the aggregation cache before it times out. The range is from 10 to 600 seconds. The default is 15 seconds.

Command Default

The operational parameters for NetFlow accounting aggregation caches are not configured.

Command Modes

NetFlow aggregation cache configuration (config-flow-cache)

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(7)T	This command function was modified to support cache entries for IPv6.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(18)SXF	This command was integrated into Cisco IOS Release 12.2(18)SXF.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You must have NetFlow accounting configured on your router before you can use this command.

Examples

The following example shows how to set the NetFlow aggregation cache entry limits and timeout values for the NetFlow protocol-port aggregation cache:

```
Router(config)# ip flow-aggregation cache protocol-port
Router(config-flow-cache)# cache entries 2046
Router(config-flow-cache)# cache timeout inactive 199
```

```
Router(config-flow-cache)# cache timeout active 45
Router(config-flow-cache)# enabled
```

Related Commands

Command	Description
enabled (aggregation cache)	Enables a NetFlow accounting aggregation cache.
export destination (aggregation cache)	Enables the exporting of NetFlow accounting information from NetFlow aggregation caches.
ip flow-aggregation cache	Enables NetFlow accounting aggregation cache schemes.
mask (IPv4)	Specifies the source or destination prefix mask for a NetFlow accounting prefix aggregation cache.
show ip cache flow	Displays a summary of the NetFlow accounting statistics.
show ip cache flow aggregation	Displays the NetFlow accounting aggregation cache statistics.
show ip cache verbose flow	Displays a detailed summary of the NetFlow accounting statistics.
show ip flow interface	Displays NetFlow accounting configuration for interfaces.

call service stop

To shut down VoIP call service on a gateway, use the **call service stop** command in voice service SIP or voice service H.323 configuration mode. To enable VoIP call service, use the **no** form of this command. To set the command to its defaults, use the **default call service stop** command

call service stop [**forced**] [**maintain-registration**]

no call service stop

default call service stop

Syntax Description

forced	(Optional) Forces the gateway to immediately terminate all in-progress calls.
maintain-registration	(Optional) Forces the gateway to remain registered with the gatekeeper.

Command Default

VoIP call service is enabled.

Command Modes

Voice service SIP configuration (conf-serv-sip)
Voice service H.323 configuration (conf-serv-h323)

Command History

Release	Modification
12.3(1)	This command was introduced.
12.4(22)T	Support for IPv6 was added.
12.4(23.08)T01	The default behavior was clarified for SIP and H.323 protocols.

Usage Guidelines

Use the **call service stop** command to shut down the SIP or H.323 services regardless of whether the **shutdown** or **no shutdown** command was configured in voice service configuration mode.

Use the **no call service stop** command to enable SIP or H.323 services regardless of whether the **shutdown** or **no shutdown** command was configured in voice service configuration mode.

Use the **default call service stop** command to set the command to its defaults. The defaults are as follows:

- Shut down SIP or H.323 service, if the **shutdown** command was configured in voice service configuration mode.
- Enable SIP or H.323 service, if the **no shutdown** command was configured in voice service configuration mode.

Examples

The following example shows SIP call service being shut down on a Cisco gateway:

```
Router> enable
Router# configure terminal
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# call service stop
```

The following example shows H.323 call service being enabled on a Cisco gateway:

```
Router> enable
Router# configure terminal
Router(config)# voice service voip
Router(conf-voi-serv)# h323
Router(conf-serv-h323)# no call service stop
```

The following example shows SIP call service being enabled on a Cisco gateway because the **no shutdown** command was configured in voice service configuration mode:

```
Router> enable
Router# configure terminal
Router(config)#voice service voip
Router(conf-voi-serv)# no shutdown
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# default call service stop
```

The following example shows H.323 call service being shut down on a Cisco gateway because the **shutdown** command was configured in voice configuration mode:

```
Router> enable
Router# configure terminal
Router(config)# voice service voip
Router(conf-voi-serv)# shutdown
Router(conf-voi-serv)# h323
Router(conf-serv-h323)# default call service stop
```

Related Commands

Command	Description
bandwidth audio as-modifier	Allows SIP SDP bandwidth-related options.
billing b-channel	Enables the H.323 gateway to access B-channel information for all H.323 calls.
outbound-proxy	Configures an outbound proxy server.
telephony-service ccm-compatible	Enables the detection of a Cisco CallManager system in the network and allows the exchange of calls.

cdma pdsn ipv6

To enable the packet data serving node (PDSN) IPv6 functionality, use the **cdma pdsn ipv6** command in global configuration mode. To disable this function, use the **no** form of the command.

cdma pdsn ipv6 ra-count *ra-value* [**ra-interval** *seconds*]

no cdma pdsn ipv6 ra-count *ra-value* [**ra-interval** *seconds*]

Syntax Description

ra-count	Routing advertisement (RA) count determines how many RAs to send to the MN.
ra-value	Number of IPv6 RAs to be sent. The range is from 1 to 5, and the default value is 1.
ra-interval	RA interval determines how often RAs are sent to the MN.
seconds	The interval between IPv6 RAs sent. The range is from 1 to 1800, and the default value is 5.

Command Default

Number of IPv6 RAs to be sent is 1.
The interval between IPv6 RAs sent is 5 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)XY	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

Usage Guidelines

If the **cdma pdsn ipv6** command is not entered and a PDSN session is brought up with IPv6, the session will be terminated and the following message displayed:

%CDMA_PDSN-3-PDSNIPV6NOTENABLED: PDSN IPv6 feature has not been enabled.

Examples

The following example illustrates how to control the number and interval of routing advertisements sent to the MN when an IPv6 session comes up:

```
router(config)# cdma pdsn ipv6 ra-count 2 ra-interval 3
```

cef table consistency-check

To enable Cisco Express Forwarding table consistency checker types and parameters, use the **cef table consistency-check** command in global configuration mode. To disable consistency checkers, use the **no** form of this command.

cef table consistency-check {**ipv4** | **ipv6**} [**type** {**lc-detect** | **scan-lc-rp** | **scan-rp-lc** | **scan-rib-ios** | **scan-ios-rib**} [**count** *count-number* [**period** *seconds*] | **period** *seconds*] | **error-message** | **auto-repair** [**delay** *seconds* [**holddown** *seconds*] | **holddown** *seconds*] | **data-checking**]

no cef table consistency-check {**ipv4** | **ipv6**} [**type** {**lc-detect** | **scan-lc-rp** | **scan-rp-lc** | **scan-rib-ios** | **scan-ios-rib**} [**count** *count-number* [**period** *seconds*] | **period** *seconds*] | **error-message** | **auto-repair** | **data-checking**]

Syntax Description

ipv4	Checks IPv4 addresses.
ipv6	Checks IPv6 addresses. **Note** On the Cisco 10000 series routers, IPv6 is supported on Cisco IOS Release 12.2(28)SB and later releases.
type	(Optional) Specifies the type of consistency check to enable.
lc-detect	(Optional) (Distributed platforms such as the Cisco 7500 series only) Detects missing prefixes on the line card. The information is confirmed by the Route Switch Processor (RSP). This consistency checker operates on the line card by retrieving IP prefixes that are missing from its Forwarding Information Base (FIB) table. If IP prefixes are missing, the line card cannot forward packets for these addresses. This consistency checker then sends IP prefixes to the RSP for confirmation. If the RSP detects that it has the relevant entry, an inconsistency is detected, and an error message is displayed. Finally, the RSP sends a signal back to the line card confirming that the IP prefix is an inconsistency.
scan-lc-rp	(Optional) (Distributed platforms only) Performs a passive scan check of tables on the line card. This consistency checker operates on the line card by examining the FIB table for a configurable time period and sending the next *x* prefixes to the RSP. The RSP does an exact lookup, and if it finds the prefix missing, it reports an inconsistency. Finally, the RSP sends a signal back to the line card for confirmation.
scan-rp-lc	(Optional) Operates on the RSP (opposite of the **scan-lc-rp** consistency checker) by examining the FIB table for a configurable time period and sending the next *x* prefixes to the line card. The line card does an exact lookup. If it finds the prefix missing, the line card reports an inconsistency and signals the RSP for confirmation.
scan-rib-ios	(Optional) Compares the Routing Information Base (RIB) to the FIB table and provides the number of entries missing from the FIB table.
scan-ios-rib	(Optional) Compares the FIB table to the RIB and provides the number of entries missing from the RIB.

count *count-number*	(Optional) Specifies the maximum number of prefixes to check per scan. The range is from 2 to 10000. The default count number is 1000 prefixes per scan for the **scan-rib-ios** and **scan-ios-rib** keywords. The default count number is 0 for the **lc-detect**, **scan-lc-rp**, and **scan-rp-lc** keywords.
period *seconds*	(Optional) Period between scans. Valid values are from 30 to 3600 seconds. The default is 60 seconds.
error-message	(Optional) Enables the consistency checker to generate an error message when it detects an inconsistency. By default, this function is disabled.
auto-repair	(Optional) Enables the auto repair function. By default, this function is enabled. You can enter the **no** form of the command to disable auto repair or enter the default form of the command to return the auto repair settings to a 10-second delay and 300-second holddown.
delay *seconds*	(Optional) Specifies how long the consistency checker waits to fix an inconsistency. The range is 10 to 300 seconds. The default delay is 10 seconds.
holddown *seconds*	(Optional) Specifies how long the consistency checker waits to reenable auto repair after auto repair runs. The range is from 300 to 3000 seconds. The default delay is 300 seconds.
data-checking	(Optional) Enables the consistency checker data-checking utility. By default, this function is disabled.

Command Default

All consistency checkers are disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(25)S	This command was introduced. This command replaces the **ip cef table consistency-check** command.
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.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
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 Router.

Examples

The following example enables the Cisco Express Forwarding consistency checker to check IPv4 addresses:

```
Router(config)# cef table consistency-check ipv4
```

The following example enables the Cisco Express Forwarding consistency checker to check IPv4 addresses and specifies the scan-rp-lc checker to run every 60 seconds for 5000 prefixes:

```
Router(config)# cef table consistency-check ipv4 type scan-rp-lc count 5000 period 60
```

The following example enables the Cisco Express Forwarding consistency checker to check IPv4 addresses and display an error message when it finds an inconsistency:

```
Router(config)# cef table consistency-check ipv4 error-message
```

Related Commands

Command	Description
clear cef table	Clears the Cisco Express Forwarding tables.
clear ip cef inconsistency	Clears Cisco Express Forwarding inconsistency statistics and records found by the Cisco Express Forwarding consistency checkers.
debug cef	Enables the display of information about Cisco Express Forwarding events.
debug ip cef table	Enables the collection of events that affect entries in the Cisco Express Forwarding tables.
show cef table consistency-check	Displays Cisco Express Forwarding consistency checker table values.
show ip cef inconsistency	Displays Cisco Express Forwarding IP prefix inconsistencies.

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).
15.1(2)T	Support for IPv6 was added.

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 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.

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.
12.2(50)SY	This command was modified. Information about IPv4 and IPv6 hardware statistics is displayed.

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 bgp ipv6

To reset IPv6 Border Gateway Protocol (BGP) sessions, use the **clear bgp ipv6** command in privileged EXEC mode.

clear bgp ipv6 {**unicast** | **multicast**} {***** | *autonomous-system-number* | *ip-address* | *ipv6-address* | *peer-group-name*} [**soft**] [**in** | **out**]

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.
*	Resets all current BGP sessions.
autonomous-system-number	Resets BGP sessions for BGP neighbors within the specified autonomous system.
ip-address	Resets the TCP connection to the specified IPv4 BGP neighbor and removes all routes learned from the connection from the BGP table.
ipv6-address	Resets the TCP connection to the specified IPv6 BGP neighbor and removes all routes learned from the connection from the BGP table. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
peer-group-name	Resets the TCP connection to the specified IPv6 BGP neighbor and removes all routes learned from the connection from the BGP table.
soft	(Optional) Soft reset. Does not reset the session.
in | **out**	(Optional) Triggers inbound or outbound soft reconfiguration. If the **in** or **out** option is not specified, both inbound and outbound soft resets are triggered.

Command Default

No reset is initiated.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)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 Release 12.2(14)S.
12.3(2)T	The **unicast** keyword was added to Cisco IOS Release 12.3(2)T.
12.0(26)S	The **unicast** and **multicast** keywords were added to Cisco IOS Release 12.0(26)S.
12.3(4)T	The **multicast** keyword was added to Cisco IOS Release 12.3(4)T.
12.2(25)S	The **multicast** keyword was added to Cisco IOS Release 12.2(25)S.

Release	Modification
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.
12.2(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.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

The **clear bgp ipv6** command is similar to the **clear ip bgp** command, except that it is IPv6-specific.

Use of the **clear bgp ipv6** command allows a reset of the neighbor sessions with varying degrees of severity depending on the specified keywords and arguments.

Use the **clear bgp ipv6 unicast** command to drop neighbor sessions with IPv6 unicast address prefixes.

The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the **unicast** keyword is mandatory starting with Cisco IOS Release 12.3(2)T.

The **multicast** keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Use the **clear bgp ipv6 *** command to drop all neighbor sessions. The Cisco IOS software will then reset the neighbor connections. Use this form of the command in the following situations:

- BGP timer specification change
- BGP administrative distance changes

Use the **clear bgp ipv6 soft out** or the **clear bgp ipv6 unicast soft out** command to drop only the outbound neighbor connections. Inbound neighbor sessions will not be reset. Use this form of the command in the following situations:

- BGP-related access lists change or get additions
- BGP-related weights change
- BGP-related distribution lists change
- BGP-related route maps change

Use the **clear bgp ipv6 soft in** or the **clear bgp ipv6 unicast soft in** command to drop only the inbound neighbor connections. Outbound neighbor sessions will not be reset. To reset inbound routing table updates dynamically for a neighbor, you must configure the neighbor to support the router refresh capability. To determine whether a BGP neighbor supports this capability, use the **show bgp ipv6 neighbors** or the **show bgp ipv6 unicast neighbors** command. If a neighbor supports the route refresh capability, the following message is displayed:

```
Received route refresh capability from peer.
```

If all BGP networking devices support the route refresh capability, use the **clear bgp ipv6** {***** | *ip-address* | *ipv6-address* | *peer-group-name*} **in** or the **clear bgp ipv6 unicast** {***** | *ip-address* | *ipv6-address* | *peer-group-name*} **in** command. Use of the **soft** keyword is not required when the route refresh capability is supported by all BGP networking devices, because the software automatically performs a soft reset.

Use this form of the command in the following situations:

- BGP-related access lists change or get additions
- BGP-related weights change
- BGP-related distribution lists change
- BGP-related route maps change

Examples

The following example clears the inbound session with the neighbor 7000::2 without the outbound session being reset:

```
Router# clear bgp ipv6 unicast 7000::2 soft in
```

The following example uses the **unicast** keyword and clears the inbound session with the neighbor 7000::2 without the outbound session being reset:

```
Router# clear bgp ipv6 unicast 7000::2 soft in
```

The following example clears the outbound session with the peer group named marketing without the inbound session being reset:

```
Router# clear bgp ipv6 unicast marketing soft out
```

The following example uses the **unicast** keyword and clears the outbound session with the peer group named peer-group marketing without the inbound session being reset:

```
Router# clear bgp ipv6 unicast peer-group marketing soft out
```

Related Commands

Command	Description
show bgp ipv6	Displays entries in the IPv6 BGP routing table.

clear bgp ipv6 dampening

To clear IPv6 Border Gateway Protocol (BGP) route dampening information and unsuppress the suppressed routes, use the **clear bgp ipv6 dampening** command in privileged EXEC mode.

clear bgp ipv6 {**unicast** | **multicast**} **dampening** [*ipv6-prefix* /*prefix-length*]

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.
ipv6-prefix	(Optional) IPv6 network about which to clear dampening information. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/*prefix-length*	(Optional) The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

Command Default

When the *ipv6-prefix*/*prefix-length* argument is not specified, the **clear bgp ipv6 dampening** command clears route dampening information for the entire IPv6 BGP routing table.

As of Cisco IOS Release 12.3(2)T, when the *ipv6-prefix*/*prefix-length* argument is not specified, the **clear bgp ipv6 unicast dampening** command clears route dampening information for the entire IPv6 BGP routing table.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)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 Release 12.2(14)S.
12.3(2)T	The **unicast** keyword was added.
12.0(26)S	The **unicast** and **multicast** keywords were added to Cisco IOS Release 12.0(26)S.
12.3(4)T	The **multicast** keyword was added to 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(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
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 introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The **clear bgp ipv6 dampening** and the **clear bgp ipv6 unicast dampening** commands are similar to the **clear ip bgp dampening** command, except they are IPv6-specific.

The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the **unicast** keyword is mandatory starting with Cisco IOS Release 12.3(2)T.

The **multicast** keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

The following example clears route dampening information about the route to network 7000::0 and unsuppresses its suppressed routes:

```
Router# clear bgp ipv6 unicast dampening 7000::/64
```

The following example uses the **unicast** keyword and clears route dampening information about the route to network 7000::0 and unsuppresses its suppressed routes:

```
Router# clear bgp ipv6 unicast dampening 7000::/64
```

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes various BGP route dampening factors.
show bgp ipv6 dampened-paths	Displays IPv6 BGP dampened routes.

clear bgp ipv6 external

To clear external IPv6 Border Gateway Protocol (BGP) peers, use the **clear bgp ipv6 external** command in privileged EXEC mode.

clear bgp ipv6 {**unicast** | **multicast**} **external** [**soft**] [**in** | **out**]

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.
soft	(Optional) Soft reset. Does not reset the session.
in | **out**	(Optional) Triggers inbound or outbound soft reconfiguration. If the **in** or **out** option is not specified, both inbound and outbound soft resets are triggered.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)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 Release 12.2(14)S.
12.3(2)T	The **unicast** keyword was added to Cisco IOS Release 12.3(2)T.
12.0(26)S	The **unicast** and **multicast** keywords were added to Cisco IOS Release 12.0(26)S.
12.3(4)T	The **multicast** keyword was added to 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(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
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 introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The **clear bgp ipv6 external** command is similar to the **clear ip bgp external** command, except that it is IPv6-specific.

The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the **unicast** keyword is mandatory starting with Cisco IOS Release 12.3(2)T.

The **multicast** keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

The following example clears the inbound session with external IPv6 BGP peers without the outbound session being reset:

```
Router# clear bgp ipv6 unicast external soft in
```

The following example uses the **unicast** keyword and clears the inbound session with external IPv6 BGP peers without the outbound session being reset:

```
Router# clear bgp ipv6 unicast external soft in
```

Related Commands

Command	Description
clear bgp ipv6	Resets an IPv6 BGP connection by dropping all neighbor sessions.

clear bgp ipv6 flap-statistics

To clear IPv6 Border Gateway Protocol (BGP) flap statistics, use the **clear bgp ipv6 flap-statistics** command in privileged EXEC mode.

clear bgp ipv6 {**unicast** | **multicast**} **flap-statistics** [*ipv6-prefix*/*prefix-length* | **regexp** *regexp* | **filter-list** *list*]

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.
ipv6-prefix	(Optional) Clears flap statistics for a single entry at this IPv6 network. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/prefix-length	(Optional) The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
regexp *regexp*	(Optional) Clears flap statistics for all the paths that match the regular expression.
filter-list *list*	(Optional) Clears flap statistics for all the paths that pass the access list. The acceptable access list number range is from 1 to 199.

Command Default

No statistics are cleared.
If no arguments or keywords are specified, the software clears flap statistics for all routes.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)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 Release 12.2(14)S.
12.3(2)T	The **unicast** keyword was added.
12.0(26)S	The **unicast** and **multicast** keywords were added to Cisco IOS Release 12.0(26)S.
12.3(4)T	The **multicast** keyword was added to 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(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
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 introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The **clear bgp ipv6 flap-statistics** command is similar to the **clear ip bgp flap-statistics** command, except that it is IPv6-specific.

The flap statistics for a route are also cleared when an IPv6 BGP peer is reset. Although the reset withdraws the route, no penalty is applied in this instance even though route flap dampening is enabled.

The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the **unicast** keyword is mandatory starting with Cisco IOS Release 12.3(2)T.

The **multicast** keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

The following example clears all of the flap statistics for paths that pass access list 3:

```
Router# clear bgp ipv6 unicast flap-statistics filter-list 3
```

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes various BGP route dampening factors.
show bgp ipv6 flap-statistics	Displays IPv6 BGP flap statistics.

clear bgp ipv6 peer-group

To clear all members of an IPv6 Border Gateway Protocol (BGP) peer group, use the **clear bgp ipv6 peer-group** command in privileged EXEC mode.

clear bgp ipv6 {**unicast** | **multicast**} **peer-group** [*name*]

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.
name	BGP peer group name.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.0(26)S	The **unicast** and **multicast** keywords were added to Cisco IOS Release 12.0(26)S.
12.3(4)T	The **unicast** and **multicast** keywords were added to Cisco IOS Release 12.3(4)T.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

Using the **clear bgp ipv6 peer-group** command without the optional *name* argument will clear all BGP peer groups.

The **multicast** keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

The following example clears all IPv6 BGP peer groups:

```
Router# clear bgp ipv6 unicast peer-group
```

clear cef table

To clear the Cisco Express Forwarding tables, use the **clear cef table** command in privileged EXEC mode.

clear cef table {**ipv4** | **ipv6**} [**vrf** {*vrf-name* | ***** }]

Syntax Description

ipv4	Clears the Cisco Express Forwarding tables for IPv4 addresses.
ipv6	Clears the Cisco Express Forwarding tables for IPv6 addresses. **Note** On the Cisco 10000 series routers IPv6 is supported on Cisco IOS Release 12.2(28)SB and later releases.
vrf	(Optional) Specifies all VPN routing and forwarding (VRF) instance tables or a specific VRF table for an IPv4 or IPv6 address.
vrf-name	(Optional) Clears the specific VRF table for IPv4 or IPv6 addresses.
*	(Optional) Clears all the VRF tables for IPv4 or IPv6 addresses.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(25)S	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.
12.2(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

The **clear cef table** command clears the selected table or address family of tables (for IPv4 or IPv6) and updates (refreshes) them throughout the router (including the Route Processor and line cards). The command increments the table epoch, updates the tables, distributes the updated information to the line cards, and performs a distributed purge of any stale entries in the tables based on the noncurrent epoch number. This ensures that any inconsistencies that occurred over time are removed.

Because this command might require significant processing resources and can cause dropped traffic or system error messages about excessive CPU use, it's use is recommended only as a last resort for debugging or mitigating serious problems.

Cisco Express Forwarding tables are also cleared automatically during bootup or online insertion and removal (OIR) of line cards.

Note On the Cisco 10000 series routers, IPv6 is supported on Cisco IOS Release 12.2(28)SB or later releases.

Examples

The following example clears the Cisco Express Forwarding tables for the IPv6 address family:

```
Router# clear cef table ipv6 vrf *
```

The following example clears the Cisco Express Forwarding tables for a VRF table named vrf1 in the IPv4 address family:

```
Router# clear cef table ipv4 vrf vrf1
```

The following example clears the Cisco Express Forwarding tables for all VRF tables in the IPv4 address family. This example shows output with Cisco Express Forwarding table debugging enabled:

```
Router# clear cef table ipv4 vrf *

06:56:01: FIBtable: Refreshing table IPv4:Default
06:56:01: FIBtable: Invalidated 224.0.0.0/4 in IPv4:Default
06:56:01: FIBtable: Deleted 224.0.0.0/4 from IPv4:Default
06:56:01: FIBtable: Validated 224.0.0.0/4 in IPv4:Default
06:56:01: FIBtable: IPv4: Event up, 10.1.41.0/24, vrf Default, 1 path, flags 0100
0220
06:56:01: FIBtable: IPv4: Adding route for 10.1.41.0/24 but route already exists.
 Trying modify.
06:56:01: FIBtable: IPv4: Event up, 10.0.0.11/32, vrf Default, 1 path, flags 010
00000
06:56:01: FIBtable: IPv4: Adding route for 10.0.0.11/32 but route already exists
. Trying modify.
06:56:01: FIBtable: IPv4: Event up, 10.0.0.15/32, vrf Default, 1 path, flags 010
00000
06:56:01: FIBtable: IPv4: Adding route for 10.0.0.15/32 but route already exists
. Trying modify.
06:56:01: FIBtable: IPv4: Event up, 10.0.0.7/32, vrf Default, 1 path, flags 0100
0220
06:56:01: FIBtable: IPv4: Adding route for 10.0.0.7/32 but route already exists.
 Trying modify.
06:56:01: FIBtable: IPv4: Event up, 10.0.0.0/8, vrf Default, 1 path, flags 00000
220
06:56:01: FIBtable: IPv4: Adding route for 10.0.0.0/8 but route already exists.
Trying modify.
06:56:01: FIBtable: IPv4: Event up, 0.0.0.0/0, vrf Default, 1 path, flags 004200
05
06:56:01: FIBtable: IPv4: Adding route for 0.0.0.0/0 but route already exists. T
rying modify.
06:56:01: FIBtable: Starting purge of table IPv4:Default to epoch 13
06:56:01: FIBtable: Invalidated 10.1.41.1/32 in IPv4:Default
06:56:01: FIBtable: Deleted 10.1.41.1/32 from IPv4:Default
06:56:01: FIBtable: Purged 1 prefix from table IPv4:Default
06:56:01: FIBtable: Validated 10.1.41.1/32 in IPv4:Default
06:56:06: FIBtable: IPv4: Event modified, 0.0.0.0/0, vrf Default, 1 path, flags
00420005
06:56:06: FIBtable: IPv4: Event up, default, 0.0.0.0/0, vrf Default, 1 path, fla
gs 00420005
06:56:06: FIBtable: IPv4: Adding route for 0.0.0.0/0 but route already exists. T
rying modify.
```

Related Commands

Command	Description
clear ip cef inconsistency	Clears Cisco Express Forwarding inconsistency statistics and records found by the Cisco Express Forwarding consistency checkers.
debug cef	Enables the display of information about Cisco Express Forwarding events.
debug ip cef table	Enables the collection of events that affect entries in the Cisco Express Forwarding tables.
show cef table consistency-check	Displays Cisco Express Forwarding consistency checker table values.
show ip cef inconsistency	Displays Cisco Express Forwarding IP prefix inconsistencies.

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 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 eigrp address-family neighbors

To delete entries from the Enhanced Interior Gateway Routing Protocol (EIGRP) neighbor table, use the **clear eigrp address-family neighbors** command in privileged EXEC mode.

clear eigrp address-family {**ipv4** [*autonomous-system-number* | **vrf** [*vrf-name*] | [*autonomous-system-number*]] | **ipv6** [*autonomous-system-number*]} **neighbors** [*ip-address*] [*interface-type interface-number*] [**soft**]

Syntax Description

ipv4	Selects neighbors formed using the IPv4 protocol family.
ipv6	Selects neighbors formed using the IPv6 protocol family.
autonomous-system-number	(Optional) Autonomous system number of the EIGRP routing process. If no autonomous system number is specified, all autonomous systems are affected.
vrf	(Optional) Deletes entries from the neighbor table for the specified IPv4 VRF.
vrf-name	(Optional) Name of the VRF address-family to which the command is applied.
ip-address	(Optional) IPv4 or IPv6 address of the neighbor. Specifying an address removes all entries with this address from the neighbor table.
interface-type	(Optional) Interface type. Specifying this argument removes the specified interface type that all entries learned via this interface from the neighbor table.
interface-number	(Optional) Interface number. Specifying this arguments removes the specified interface number that all entries learned via this interface from the neighbor table.
soft	(Optional) Gracefully informs the peer that adjacency is being resynced. This method does not take the peer down and back up with a hard reset.

Command Default

Entries in the EIGRP neighbor table are not cleared.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

Caution This command causes peers to bounce and routes to be relearned. Use this command only with the guidance of Cisco technical support.

Specifying the *interface-type* and *interface-number* arguments clears the neighbors on the specified interface from the neighbor table.

Specifying the VRF for an IPv4 address family clears neighbors in that VRF only. If an autonomous-system number is provided along with the VRF, then only the neighbors of that autonomous-system number in the VRF are cleared.

Examples

The following example removes the neighbor whose address is 172.16.8.3:

```
Router# clear eigrp address-family ipv4 neighbors 172.16.8.3
```

The following example clears EIGRP neighbors reached through the VRF named VRF1 in autonomous system 101:

```
Router# clear eigrp address-family ipv4 vrf VRF1 101 neighbors
```

The following example clears EIGRP neighbors reached through the VRF named VRF1 in autonomous system 101 learned through Ethernet interface 0/0:

```
Router# clear eigrp address-family ipv4 vrf VRF1 101 neighbors ethernet0/0
```

Related Commands

Command	Description
clear eigrp topology	Clears an EIGRP process for a topology instance.
clear ip eigrp neighbors	Deletes entries from the EIGRP neighbor table.
show eigrp address-family neighbors	Displays neighbors discovered by EIGRP.
show ip eigrp address-family neighbors	Displays neighbors discovered by EIGRP.

clear frame-relay-inarp

To clear dynamically created Frame Relay maps, which are created by the use of Inverse Address Resolution Protocol (ARP), use the **clear frame-relay-inarp** command in privileged EXEC mode.

clear frame-relay-inarp

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 12.2(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 dynamically created Frame Relay maps:

```
clear frame-relay-inarp
```

Related Commands

Command	Description
frame-relay inverse-arp	Reenables Inverse ARP on a specified interface or subinterface.
show frame-relay map	Displays the current map entries and information about the connections.

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.
12.2(50)SY	This command was modified. Information about IPv4 and IPv6 hardware statistics is displayed.

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 ipv6 access-list

To reset the IPv6 access list match counters, use the **clear ipv6 access-list** command in privileged EXEC mode.

clear ipv6 access-list [*access-list-name*]

Syntax Description

access-list-name	(Optional) Name of the IPv6 access list for which to clear the match counters. Names cannot contain a space or quotation mark, or begin with a numeric.

Command Default

No reset is initiated.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(23)S	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(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 introduced on Cisco ASR 1000 Series Routers.
12.2(50)SY	This command was modified. Information about IPv4 and IPv6 hardware statistics is displayed.

Usage Guidelines

The **clear ipv6 access-list** command is similar to the **clear ip access-list counters** command, except that it is IPv6-specific.

The **clear ipv6 access-list** command used without the *access-list-name* argument resets the match counters for all IPv6 access lists configured on the router.

This command resets the IPv6 global ACL hardware counters.

Examples

The following example resets the match counters for the IPv6 access list named marketing:

```
Router# clear ipv6 access-list marketing
```

Related Commands

Command	Description
hardware statistics	Enables the collection of hardware statistics.

ipv6 access-list	Defines an IPv6 access list and enters IPv6 access list configuration mode.
show ipv6 access-list	Displays the contents of all current IPv6 access lists.

clear ipv6 dhcp

To clear IPv6 Dynamic Host Configuration Protocol (DHCP) information, use the **clear ipv6 dhcp** command in privileged EXEC mode:

clear ipv6 dhcp

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.

Usage Guidelines

The **clear ipv6 dhcp** command deletes DHCP for IPv6 information.

Examples

The following example:

```
Router# clear ipv6 dhcp
```

clear ipv6 dhcp binding

To delete automatic client bindings from the Dynamic Host Configuration Protocol (DHCP) for IPv6 server binding table, use the **clear ipv6 dhcp binding** command in privileged EXEC mode.

clear ipv6 dhcp binding [*ipv6-address*] [**vrf** *vrf-name*]

Syntax Description

ipv6-address	(Optional) The address of a DHCP for IPv6 client. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.4(24)T	This command was modified. It was updated to allow for clearing all address bindings associated with a client.
Cisco IOS XE Release 2.1	This command was implemented on Cisco ASR 1000 Series Routers.
12.2(33)XNE	It was integrated into Cisco IOS Release 12.2(33)SXE.
15.1(2)S	This command was modified. The **vrf** *vrf-name* keyword and argument were added.
Cisco IOS XE Release 3.3S	This command was modified. The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

The **clear ipv6 dhcp binding** command is used as a server function.

A binding table entry on the DHCP for IPv6 server is automatically:

- Created whenever a prefix is delegated to a client from the configuration pool.
- Updated when the client renews, rebinds, or confirms the prefix delegation.
- Deleted when the client releases all the prefixes in the binding voluntarily, all prefixes' valid lifetimes have expired, or an administrator runs the **clear ipv6 dhcp binding** command.

If the **clear ipv6 dhcp binding** command is used with the optional *ipv6-address* argument specified, only the binding for the specified client is deleted. If the **clear ipv6 dhcp binding** command is used without the *ipv6-address* argument, then all automatic client bindings are deleted from the DHCP for IPv6 binding table. If the optional **vrf** *vrf-name* keyword and argument combination is used, only the bindings for the specified VRF are cleared.

Examples

The following example deletes all automatic client bindings from the DHCP for IPv6 server binding table:

```
Router# clear ipv6 dhcp binding
```

Related Commands

Command	Description
show ipv6 dhcp binding	Displays automatic client bindings from the DHCP for IPv6 server binding table.

clear ipv6 dhcp client

To restart the Dynamic Host Configuration Protocol (DHCP) for IPv6 client on an interface, use the **clear ipv6 dhcp client** command in privileged EXEC mode.

clear ipv6 dhcp client *interface-type interface-number*

Syntax Description

interface-type interface-number	Interface type and number. For more information, use the question mark (**?**) online help function.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SXE.

Usage Guidelines

The **clear ipv6 dhcp client** command restarts the DHCP for IPv6 client on specified interface after first releasing and unconfiguring previously acquired prefixes and other configuration options (for example, Domain Name System [DNS] servers).

Examples

The following example restarts the DHCP for IPv6 client for Ethernet interface 1/0:

```
Router# clear ipv6 dhcp client Ethernet 1/0
```

Related Commands

Command	Description
show ipv6 dhcp interface	Displays DHCP for IPv6 interface information.

clear ipv6 dhcp conflict

To clear an address conflict from the Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server database, use the **clear ipv6 dhcp conflict** command in privileged EXEC mode.

clear ipv6 dhcp conflict {***** | *ipv6-address* | **vrf** *vrf-name*}

Syntax Description

*****	Clears all address conflicts.
ipv6-address	Clears the host IPv6 address that contains the conflicting address.
vrf *vrf-name*	Specifies a virtual routing and forwarding (VRF) name.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(24)T	This command was introduced.
15.1(2)S	This command was modified. The **vrf** *vrf-name* keyword and argument were added.
Cisco IOS XE Release 3.3S	This command was modified. The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

When you configure the DHCPv6 server to detect conflicts, it uses ping. The client uses neighbor discovery to detect clients and reports to the server through a DECLINE message. If an address conflict is detected, the address is removed from the pool, and the address is not assigned until the administrator removes the address from the conflict list.

If you use the asterisk (*) character as the address parameter, DHCP clears all conflicts.

If the **vrf** *vrf-name* keyword and argument are specified, only the address conflicts that belong to the specified VRF will be cleared.

Examples

The following example shows how to clear all address conflicts from the DHCPv6 server database:

```
Router# clear ipv6 dhcp conflict *
```

Related Commands

Command	Description
show ipv6 dhcp conflict	Displays address conflicts found by a DHCPv6 server when addresses are offered to the client.

clear ipv6 dhcp relay binding

To clear a specific Dynamic Host Configuration Protocol (DHCP) for IPv6 relay binding, use the **clear ipv6 dhcp relay binding** command in privileged EXEC mode.

clear ipv6 dhcp relay binding [*ipv6-address* | **vrf** *vrf-name*]

Syntax Description

ipv6-address	(Optional) The address of a DHCP for IPv6 relay client.
vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.
15.1(2)S	This command was modified. The **vrf** *vrf-name* keyword and argument were added.
Cisco IOS XE Release 3.3S	This command was modified. The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

The **clear ipv6 dhcp relay binding** command deletes only the binding for the specified relay client. If no relay client is specified, no binding is deleted.

Examples

The following example clears the binding for the client with the specified IPv6 address:

```
Router# clear ipv6 dhcp relay binding 2001:0DB8:3333:4::5
```

Related Commands

Command	Description
ipv6 flowset	Configures flow-label marking in 1280-byte or larger packets sent by the router.

clear ipv6 eigrp

To delete entries from Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 routing tables, use the **clear ipv6 eigrp** command in privileged EXEC mode.

clear ipv6 eigrp [*as-number*] [**neighbor** [*ipv6-address* | *interface-type interface-number*]]

Syntax Description

as-number	(Optional) Autonomous system number.
neighbor	(Optional) Deletes neighbor router entries.
ipv6-address	(Optional) IPv6 address of a neighboring router.
interface-type	(Optional) The interface type of the neighbor router.
interface-number	(Optional) The interface number of the neighbor router.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(6)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 introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

Use the **clear ipv6 eigrp** command without any arguments or keywords to clear all EIGRP for IPv6 routing table entries. Use the *as-number* argument to clear routing table entries on a specified process, and use the **neighbor** *ipv6-address* keyword and argument, or the *interface-type interface-number* argument, to remove a specific neighbor from the neighbor table.

Examples

The following example removes the neighbor whose IPv6 address is 3FEE:12E1:2AC1:EA32:

```
Router# clear ipv6 eigrp neighbor 3FEE:12E1:2AC1:EA32
```

clear ipv6 flow stats

To clear the NetFlow switching statistics, use the **clear ipv6 flow stats** command in privileged EXEC mode.

clear ipv6 flow stats

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)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

The **show iv6 cache flow** command displays the NetFlow switching statistics. Use the **clear ipv6 flow stats** command to clear the NetFlow switching statistics.

Examples

The following example clears the NetFlow switching statistics on the router:

```
Router# clear ipv6 flow stats
```

Related Commands

Command	Description
show ipv6 flow cache	Displays the routing table cache used to fast switch IPv6 traffic.

clear ipv6 inspect

To remove a specific IPv6 session or all IPv6 inspection sessions, use the **clear ipv6 inspect** command in privileged EXEC mode.

clear ipv6 inspect {**session** *session-number* | **all**}

Syntax Description

session *session-number*	Indicates the number of the session to clear.
all	Clears all inspection sessions.

Command Default

Inspection sessions previously configured are unaffected.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(7)T	This command was introduced.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Examples

The following example clears all inspection sessions:

```
Router# clear ipv6 inspect all
```

Related Commands

Command	Description
ipv6 inspect name	Applies a set of inspection rules to an interface.

clear ipv6 mfib counters

To reset all active Multicast Forwarding Information Base (MFIB) traffic counters, use the **clear ipv6 mfib counters** command in privileged EXEC mode.

clear ipv6 mfib [**vrf** *vrf-name*] **counters** [*group-name* | *group-address* [*source-address* | *source-name*]]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
group-name | *group-address*	(Optional) IPv6 address or name of the multicast group.
source-address | *source-name*	(Optional) IPv6 address or name of the source.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)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 introduced on Cisco ASR 1000 Series Routers.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

After you enable the **clear ipv6 mfib counters** command, you can determine if additional traffic is forwarded by using one of the following show commands that display traffic counters:

- **show ipv6 mfib**
- **show ipv6 mfib active**
- **show ipv6 mfib count**
- **show ipv6 mfib interface**
- **show ipv6 mfib summary**

Examples

The following example clears and resets all MFIB traffic counters:

```
Router# clear ipv6 mfib counters
```

clear ipv6 mld counters

To clear the Multicast Listener Discovery (MLD) interface counters, use the **clear ipv6 mld counters** command in privileged EXEC mode.

clear ipv6 mld [**vrf** *vrf-name*] **counters** [*interface-type*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
interface-type	(Optional) Interface type. For more information, use the question mark (**?**) online help function.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.3(4)T	This command was 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(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
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 introduced on Cisco ASR 1000 Series Routers.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

Use the **clear ipv6 mld counters** command to clear the MLD counters, which keep track of the number of joins and leaves received. If you omit the optional *interface-type* argument, the **clear ipv6 mld counters** command clears the counters on all interfaces.

Examples

The following example clears the counters for Ethernet interface 1/0:

```
Router# clear ipv6 mld counters Ethernet1/0
```

Related Commands

Command	Description
show ipv6 mld interface	Displays multicast-related information about an interface.

clear ipv6 mld traffic

To reset the Multicast Listener Discovery (MLD) traffic counters, use the **clear ipv6 mld traffic** command in privileged EXEC mode.

clear ipv6 mld [**vrf** *vrf-name*] **traffic**

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
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 introduced on Cisco ASR 1000 Series Routers.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

Using the **clear ipv6 mld traffic** command will reset all MLD traffic counters.

Examples

The following example resets the MLD traffic counters:

```
Router# clear ipv6 mld traffic
```

Syntax Description

Command	Description
show ipv6 mld traffic	Displays the MLD traffic counters.

clear ipv6 mobile binding

To clear the Mobile IPv6 binding cache on a router, use the **clear ipv6 mobile binding** command in privileged EXEC mode.

clear ipv6 mobile binding [**care-of-address** *prefix* | **home-address** *prefix* | *interface-type interface-number*]

Syntax Description

care-of-address	(Optional) Provides information about the mobile node's current location.
prefix	(Optional) IPv6 address prefix of the care-of address or the home address.
home-address	(Optional) IPv6 address assigned to the mobile node within its home subnet prefix on its home link.
interface-type interface-number	(Optional) Interface type and number.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

The **clear ipv6 mobile binding** command clears the binding caches for a specified mobile node (if specified) or all mobile nodes (if no arguments or keywords are specified).

The *prefix* argument can be a prefix for the care-of address or the home address of a mobile node, so that entire networks can be cleared. Enter **/128** to clear an individual mobile node.

Use of this command with the *interface-type* and *interface-number* arguments clears all bindings on the specified interface.

Examples

In the following example, the binding caches for all mobile nodes are cleared:

```
Router# clear ipv6 mobile binding

Clear 1 bindings [confirm]

Router# show ipv6 mobile binding

Mobile IPv6 Binding Cache Entries:

Selection matched 0 bindings
```

Related Commands

Command	Description
binding	Configures binding options for the Mobile IPv6 home agent feature in home agent configuration mode.
ipv6 mobile home-agent (global configuration)	Enters home agent configuration mode.
show ipv6 mobile binding	Displays information about the binding cache.

clear ipv6 mobile home-agents

To clear the neighboring home agents list, use the **clear ipv6 mobile home-agents** command in privileged EXEC mode.

clear ipv6 mobile home-agents [*interface-type interface-number*]

Syntax Description

interface-type interface-number	(Optional) Interface type and number.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

The **clear ipv6 mobile home-agents** command clears the neighboring home agents list. The list is subsequently reconstructed from received router advertisements.

If you do not enter the optional *interface-type* and *interface-number* arguments, the home agent lists on all interfaces are cleared.

Examples

In the following example, the neighboring home agent lists are cleared:

```
Router# clear ipv6 mobile home-agents
```

Related Commands

Command	Description
binding	Configures binding options for the Mobile IPv6 home agent feature in home agent configuration mode.
ipv6 mobile home-agent (global configuration)	Enters home agent configuration mode.
show ipv6 mobile home-agent	Displays neighboring home agents.

clear ipv6 mobile traffic

To clear statistics associated with Mobile IPv6 traffic, use the **clear ipv6 mobile traffic** command in privileged EXEC mode.

clear ipv6 mobile traffic

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.

Usage Guidelines

The **clear ipv6 mobile traffic** command clears the statistics about the received binding updates and transmitted binding acknowledgments on a mobile node.

Examples

In the following example, statistics about binding updates and binding acknowledgments are cleared:

```
Router# clear ipv6 mobile traffic

Router# show ipv6 mobile traffic

MIPv6 statistics:
  Rcvd: 0 total
      0 truncated, 0 format errors
      0 checksum errors
    Binding Updates received:0
      0 no HA option, 0 BU's length
      0 options' length, 0 invalid CoA
  Sent: 0 generated
    Binding Acknowledgements sent:0
      0 accepted (0 prefix discovery required)
      0 reason unspecified, 0 admin prohibited
      0 insufficient resources, 0 home reg not supported
      0 not home subnet, 0 not home agent for node
      0 DAD failed, 0 sequence number
    Binding Errors sent:0
      0 no binding, 0 unknown MH
```

```
Home Agent Traffic:
  0 registrations, 0 deregistrations
  unknown time since last accepted HA registration
  unknown time since last failed HA registration
  unknown last failed registration code
  Traffic forwarded:
    0 tunneled, 0 reversed tunneled
  Dynamic Home Agent Address Discovery:
    0 requests received, 0 replies sent
  Mobile Prefix Discovery:
    0 solicitations received, 0 advertisements sent
```

Related Commands

Command	Description
binding	Configures binding options for the Mobile IPv6 home agent feature in home agent configuration mode.
show ipv6 mobile home-agent	Displays neighboring home agents.

clear ipv6 mtu

To clear the maximum transmission unit (MTU) cache of messages, use the **clear ipv6 mtu** command in privileged EXEC mode.

clear ipv6 mtu

Syntax Description

This command has no arguments or keywords.

Command Default

Messages are not cleared from the MTU cache.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.

Usage Guidelines

If a router is flooded with ICMPv6 toobig messages, the router is forced to create an unlimited number of entries in the MTU cache until all available memory is consumed. Use the **clear ipv6 mtu** command to clear messages from the MTU cache.

Examples

The following example clears the MTU cache of messages:

```
Router# clear ipv6 mtu
```

Related Commands

Command	Description
ipv6 flowset	Configures flow-label marking in 1280-byte or larger packets sent by the router.

clear ipv6 multicast aaa authorization

To clear authorization parameters that restrict user access to an IPv6 multicast network, use the **clear ipv6 multicast aaa authorization** command in privileged EXEC mode.

clear ipv6 multicast aaa authorization [*interface-type interface-number*]

Syntax Description

interface-type interface-number	Interface type and number. For more information, use the question mark (**?**) online help function.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

Using the **clear ipv6 multicast aaa authorization** command without the optional *interface-type* and *interface-number* arguments will clear all authorization parameters on a network.

Examples

The following example clears all configured authorization parameters on an IPv6 network:

```
Router# clear ipv6 multicast aaa authorization FastEthernet 1/0
```

Related Commands

Command	Description
aaa authorization multicast default	Sets parameters that restrict user access to an IPv6 multicast network.

clear ipv6 nat translation

To clear dynamic Network Address Translation—Protocol Translation (NAT-PT) translations from the dynamic state table, use the **clear ipv6 nat translation** command in privileged EXEC mode.

clear ipv6 nat translation *

Syntax Description

*	Clears all dynamic NAT-PT translations.

Command Default

Entries are deleted from the dynamic translation state table when they time out.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

Use this command to clear entries from the dynamic translation state table before they time out. Static translation configuration is not affected by this command.

Examples

The following example shows the NAT-PT entries before and after the dynamic translation state table is cleared. Note that all the dynamic NAT-PT mappings are cleared, but the static NAT-PT configurations remain.

```
Router# show ipv6 nat translations

Prot  IPv4 source              IPv6 source
      IPv4 destination         IPv6 destination
---   ---                      ---
      192.168.123.2            2001::2

---   ---                      ---
      192.168.122.10           2001::10

tcp   192.168.124.8,11047      3002::8,11047
      192.168.123.2,23         2001::2,23

udp   192.168.124.8,52922      3002::8,52922
      192.168.123.2,69         2001::2,69

Router# clear ipv6 nat translation *
```

```
Router# show ipv6 nat translations

Prot  IPv4 source              IPv6 source
      IPv4 destination         IPv6 destination
---   ---                      ---
      192.168.123.2            2001::2

---   ---                      ---
      192.168.122.10           2001::10
```

Related Commands

Command	Description
ipv6 nat	Designates that traffic originating from or destined for the interface is subject to NAT-PT.
show ipv6 nat translations	Displays active NAT-PT translations.

clear ipv6 neighbors

To delete all entries in the IPv6 neighbor discovery cache, except static entries, use the **clear ipv6 neighbors** command in privileged EXEC mode.

Syntax for Releases 15.0(1)M, 12.2(33)SXH, and 12.2(33)SRC, and Later Releases

clear ipv6 neighbors [**interface** *type number* [**ipv6** *ipv6-address*] | **statistics** | **vrf** *table-name* [*ipv6-address* | **statistics**]]

Syntax for Release Cisco IOS XE Release 2.1 and Later Releases

clear ipv6 neighbors

Syntax Description

interface *type number*	(Optional) Clears the IPv6 neighbor discovery cache in the specified interface.
ipv6 *ipv6-address*	(Optional) Clears the IPv6 neighbor discovery cache that matches the specified IPv6 address on the specified interface.
statistics	(Optional) Clears the IPv6 neighbor discovery entry cache.
vrf	(Optional) Clears entries for a virtual private network (VPN) routing or forwarding instance.
table-name	(Optional) Table name or identifier. The value range is from 0x0 to 0xFFFFFFFF (0 to 65535 in decimal).

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)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 Release 12.2(14)S.
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.
12.2(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.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The **vrf** keyword and *table-name* argument were added.
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 implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Examples

The following example deletes all entries, except static entries, in the neighbor discovery cache:

```
Router# clear ipv6 neighbors
```

The following example clears all IPv6 neighbor discovery cache entries, except static entries, on Ethernet interface 0/0:

```
Router# clear ipv6 neighbors interface Ethernet 0/0
```

The following examples clears a neighbor discovery cache entry for 2001:0DB8:1::1 on Ethernet interface 0/0:

```
Router# clear ipv6 neighbors interface Ethernet0/0 ipv6 2001:0DB8:1::1
```

Related Commands

Command	Description
ipv6 neighbor	Configures a static entry in the IPv6 neighbor discovery cache.
show ipv6 neighbors	Displays IPv6 neighbor discovery cache information.

clear ipv6 nhrp

To clear all dynamic entries from the Next Hop Resolution Protocol (NHRP) cache, use the **clear ipv6 nhrp** command in privileged EXEC mode.

clear ipv6 nhrp [*ipv6-address* | **counters**]

Syntax Description

ipv6-address	(Optional) The IPv6 network to delete.
counters	(Optional) Specifies NHRP counters to delete.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

This command does not clear any static (configured) IPv6-to-nonbroadcast multiaccess (NBMA) address mappings from the NHRP cache.

Examples

The following example shows how to clear all dynamic entries from the NHRP cache for the interface:

```
Router# clear ipv6 nhrp
```

Related Commands

Command	Description
show ipv6 nhrp	Displays the NHRP cache.

clear ipv6 ospf

To clear the Open Shortest Path First (OSPF) state based on the OSPF routing process ID, use the **clear ipv6 ospf** command in privileged EXEC mode.

clear ipv6 ospf [*process-id*] {**process** | **force-spf** | **redistribution**}

Syntax Description

process-id	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when enabling the OSPF routing process.
process	Restarts the OSPF process.
force-spf	Starts the shortest path first (SPF) algorithm without first clearing the OSPF database.
redistribution	Clears OSPF route redistribution.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)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.
15.0(1)M	This command was integrated into Cisco IOS Release 12.5(1)M.

Usage Guidelines

When the **process** keyword is used with the **clear ipv6 ospf** command, the OSPF database is cleared and repopulated, and then the shortest path first (SPF) algorithm is performed. When the **force-spf** keyword is used with the **clear ipv6 ospf** command, the OSPF database is not cleared before the SPF algorithm is performed.

Use the *process-id* option to clear only one OSPF process. If the *process-id* option is not specified, all OSPF processes are cleared.

Examples

The following example starts the SPF algorithm without clearing the OSPF database:

```
Router# clear ipv6 ospf force-spf
```

clear ipv6 ospf counters

To clear the Open Shortest Path First (OSPF) state based on the OSPF routing process ID, use the **clear ipv6 ospf** command in privileged EXEC mode.

clear ipv6 ospf [*process-id*] **counters** [**neighbor** [*neighbor-interface* | *neighbor-id*]]

Syntax Description

process-id	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when enabling the OSPF routing process.
neighbor	(Optional) Neighbor statistics per interface or neighbor ID.
neighbor-interface	(Optional) Neighbor interface.
neighbor-id	(Optional) IPv6 or IP address of the neighbor.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)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.

Usage Guidelines

Use the **neighbor** *neighbor-interface* option to clear counters for all neighbors on a specified interface. If the **neighbor** *neighbor-interface* option is not used, all OSPF counters are cleared.

Use the **neighbor** *neighbor-id* option to clear counters at a specified neighbor. If the **neighbor** *neighbor-id* option is not used, all OSPF counters are cleared.

Examples

The following example provides detailed information on a neighbor router:

```
Router# show ipv6 ospf neighbor detail

 Neighbor 10.0.0.1
    In the area 1 via interface Serial19/0
    Neighbor:interface-id 21, link-local address FE80::A8BB:CCFF:FE00:6F00
    Neighbor priority is 1, State is FULL, 6 state changes
    Options is 0x194AE05
    Dead timer due in 00:00:37
    Neighbor is up for 00:00:15
    Index 1/1/1, retransmission queue length 0, number of retransmission 1
    First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
    Last retransmission scan length is 1, maximum is 1
    Last retransmission scan time is 0 msec, maximum is 0 msec
```

The following example clears all neighbors on the specified interface:

```
Router# clear ipv6 ospf counters neighbor s19/0
```

The following example now shows that there have been 0 state changes since the **clear ipv6 ospf counters neighbor s19/0** command was used:

```
Router# show ipv6 ospf neighbor detail

 Neighbor 10.0.0.1
    In the area 1 via interface Serial19/0
    Neighbor:interface-id 21, link-local address FE80::A8BB:CCFF:FE00:6F00
    Neighbor priority is 1, State is FULL, 0 state changes
    Options is 0x194AE05
    Dead timer due in 00:00:39
    Neighbor is up for 00:00:43
    Index 1/1/1, retransmission queue length 0, number of retransmission 1
    First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
    Last retransmission scan length is 1, maximum is 1
    Last retransmission scan time is 0 msec, maximum is 0 msec
```

Related Commands

Command	Description
show ipv6 ospf neighbor	Displays OSPF neighbor information on a per-interface basis.

clear ipv6 ospf events

To clear the Open Shortest Path First (OSPF) for IPv6 event log content based on the OSPF routing process ID, use the **clear ipv6 ospf events** command in privileged EXEC mode.

clear ipv6 ospf [*process-id*] **events**

Syntax Description

process-id	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when enabling the OSPF routing process.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 series routers.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

Use the optional *process-id* argument to clear the IPv6 event log content of a specified OSPF routing process. If the *process-id* argument is not used, all event log content is cleared.

Examples

The following example enables the clearing of OSPF for IPv6 event log content for routing process 1:

```
Router# clear ipv6 ospf 1 events
```

clear ipv6 pim counters

To reset the Protocol Independent Multicast (PIM) traffic counters, use the **clear ipv6 pim counters** command in privileged EXEC mode.

clear ipv6 pim counters

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.3(4)T	This command was 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(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
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 introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

Using the **clear ipv6 pim counters** command will reset all PIM traffic counters.

Examples

The following example resets the PIM traffic counters:

```
Router# clear ipv6 pim counters
```

Related Commands

Command	Description
show ipv6 pim traffic	Displays the PIM traffic counters.

clear ipv6 pim limit

To clear Protocol Independent Multicast (PIM) statistics, use the **clear ipv6 pim limit** command in privileged EXEC mode.

clear ipv6 pim [**vrf** *vrf-name*] **limit** [*interface*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
interface	(Optional) Specific interface for which statistics will be cleared.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

The **clear ipv6 pim limit** command clears IPv6 PIM interface statistics. If the optional *interface* argument is enabled, only statistics for the specified interface are cleared.

Examples

The following example clears PIM interface limit statistics:

```
Router# clear ipv6 pim limit
```

Related Commands

Command	Description
ipv6 multicast limit	Configures per-interface mroute state limiters in IPv6.
ipv6 multicast limit cost	Applies a cost to mroutes that match per interface mroute state limiters in IPv6.

clear ipv6 pim reset

To delete all entries from the topology table and reset the Multicast Routing Information Base (MRIB) connection, use the **clear ipv6 pim reset** command in privileged EXEC mode.

clear ipv6 pim [**vrf** *vrf-name*] **reset**

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)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.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

Using the **clear ipv6 pim reset** command breaks the PIM-MRIB connection, clears the topology table, and then reestablishes the PIM-MRIB connection. This procedure forces MRIB resynchronization.

Caution Use the **clear ipv6 pim reset** command with caution, as it clears all PIM protocol information from the PIM topology table. Use of the **clear ipv6 pim reset** command should be reserved for situations where PIM and MRIB communication are malfunctioning.

Examples

The following example deletes all entries from the topology table and resets the MRIB connection:

```
Router# clear ipv6 pim reset
```

clear ipv6 pim topology

To clear the Protocol Independent Multicast (PIM) topology table, use the **clear ipv6 pim topology** command in privileged EXEC mode.

clear ipv6 pim [**vrf** *vrf-name*] **topology** [*group-name* | *group-address*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
group-name | *group-address*	(Optional) IPv6 address or name of the multicast group.

Command Default

When the command is used with no arguments, all group entries located in the PIM topology table are cleared of PIM protocol information.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
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.
12.2(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 introduced on Cisco ASR 1000 Series Routers.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

This command clears PIM protocol information from all group entries located in the PIM topology table. Information obtained from the MRIB table is retained. If a multicast group is specified, only those group entries are cleared.

Examples

The following example clears all group entries located in the PIM topology table:

```
Router# clear ipv6 pim topology
```

clear ipv6 pim traffic

To clear the Protocol Independent Multicast (PIM) traffic counters, use the **clear ipv6 pim traffic** command in privileged EXEC mode.

clear ipv6 pim [**vrf** *vrf-name*] **traffic**

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Default

When the command is used with no arguments, all traffic counters are cleared.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(4)M	This command was introduced.

Usage Guidelines

This command clears PIM traffic counters. If the **vrf** *vrf-name* keyword and argument are used, only those counters are cleared.

Examples

The following example clears all PIM traffic counter:

```
Router# clear ipv6 pim traffic
```

clear ipv6 prefix-list

To reset the hit count of the IPv6 prefix list entries, use the **clear ipv6 prefix-list** command in privileged EXEC mode.

clear ipv6 prefix-list [*prefix-list-name*] [*ipv6-prefix*/*prefix-length*]

Syntax Description

prefix-list-name	(Optional) The name of the prefix list from which the hit count is to be cleared.
ipv6-prefix	(Optional) The IPv6 network from which the hit count is to be cleared. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/*prefix-length*	(Optional) The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

Command Default

The hit count is automatically cleared for all IPv6 prefix lists.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)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 Release 12.2(14)S.
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.
12.2(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 introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The **clear ipv6 prefix-list** command is similar to the **clear ip prefix-list** command, except that it is IPv6-specific.

The hit count is a value indicating the number of matches to a specific prefix list entry.

Examples

The following example clears the hit count from the prefix list entries for the prefix list named first_list that match the network mask 2001:0DB8::/35.

```
Router# clear ipv6 prefix-list first_list 2001:0DB8::/35
```

Related Commands

Command	Description
ipv6 prefix-list	Creates an entry in an IPv6 prefix list.
ipv6 prefix-list sequence-number	Enables the generation of sequence numbers for entries in an IPv6 prefix list.
show ipv6 prefix-list	Displays information about an IPv6 prefix list or prefix list entries.

clear ipv6 rip

To delete routes from the IPv6 Routing Information Protocol (RIP) routing table, use the **clear ipv6 rip** command in privileged EXEC mode.

clear ipv6 rip [*name*]

Syntax Description

name	(Optional) Name of an IPv6 RIP process.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(22)S	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(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.
12.2(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

When the *name* argument is specified, only routes for that process are deleted from the IPv6 RIP routing table and, if installed, from the IPv6 routing table. If no *name* argument is specified, all IPv6 RIP routes are deleted.

Use the **show ipv6 rip** command to display IPv6 RIP routes.

Examples

The following example deletes all the IPv6 routes for the RIP process called one:

```
Router# clear ipv6 rip one
```

Related Commands

Command	Description
show ipv6 rip	Displays the current contents of the IPv6 RIP routing table.

clear ipv6 route

To delete routes from the IPv6 routing table, use the **clear ipv6 route** command in privileged EXEC mode.

clear ipv6 route {*ipv6-address* | *ipv6-prefix*/*prefix-length* | *}

Syntax Description

ipv6-address	The address of the IPv6 network to delete from the table. 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	The IPv6 network number to delete from the table. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/*prefix-length*	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
*	Clears all IPv6 routes.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)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 Release 12.2(14)S.
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.
12.2(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 **clear ipv6 route** command is similar to the **clear ip route** command, except that it is IPv6-specific.

When the *ipv6-address* or *ipv6-prefix*/*prefix-length* argument is specified, only that route is deleted from the IPv6 routing table. When the * keyword is specified, all routes are deleted from the routing table (the per-destination maximum transmission unit [MTU] cache is also cleared).

Examples

The following example deletes the IPv6 network 2001:0DB8::/35:

```
Router# clear ipv6 route 2001:0DB8::/35
```

Related Commands

Command	Description
ipv6 route	Establishes static IPv6 routes.
show ipv6 route	Displays the current contents of the IPv6 routing table.

clear ipv6 snooping counters

To remove counter entries, use the **clear ipv6 snooping counters** command in privileged EXEC mode.

clear ipv6 snooping counters [**interface** *type number*]

Syntax Description

interface *type number*	(Optional) Clears the counter of entries that match the specified interface type and number.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

The **clear ipv6 snooping counters** command removes counters from all the configured interfaces. You can use the optional **interface** *type number* keyword and argument to remove counters from the specified interface.

Examples

The following example shows how to remove entries from the counter:

```
Router# clear ipv6 snooping counters
```

clear ipv6 spd

To clear the most recent Selective Packet Discard (SPD) state transition, use the **clear ipv6 spd** command in privileged EXEC mode.

clear ipv6 spd

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 **clear ipv6 spd** command removes the most recent SPD state transition and any trend historical data.

Examples

The following example shows how to clear the most recent SPD state transition:

```
Router# clear ipv6 spd
```

clear ipv6 traffic

To reset IPv6 traffic counters, use the **clear ipv6 traffic** command in privileged EXEC mode.

clear ipv6 traffic [*interface-type interface-number]*

Syntax Description

interface-type interface-number	Interface type and number. For more information, use the question mark (**?**) online help function.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)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 and output fields were added.
12.2(13)T	The modification to add output fields was integrated into this release.
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.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
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.
12.2(33)XN	The optional *interface-type* and *interface-number* arguments were added.

Usage Guidelines

Using this command resets the counters in the output from the **show ipv6 traffic** command.

Examples

The following example resets the IPv6 traffic counters. The output from the **show ipv6 traffic** command shows that the counters are reset:

```
Router# clear ipv6 traffic

Router# show ipv6 traffic

IPv6 statistics:
  Rcvd:  1 total, 1 local destination
         0 source-routed, 0 truncated
         0 format errors, 0 hop count exceeded
         0 bad header, 0 unknown option, 0 bad source
         0 unknown protocol, 0 not a router
         0 fragments, 0 total reassembled
         0 reassembly timeouts, 0 reassembly failures
  Sent:  1 generated, 0 forwarded
         0 fragmented into 0 fragments, 0 failed
         0 encapsulation failed, 0 no route, 0 too big
  Mcast: 0 received, 0 sent
```

```
ICMP statistics:
  Rcvd: 1 input, 0 checksum errors, 0 too short
        0 unknown info type, 0 unknown error type
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 0 router advert, 0 redirects
        0 neighbor solicit, 1 neighbor advert
Sent: 1 output
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 0 router advert, 0 redirects
        0 neighbor solicit, 1 neighbor advert

UDP statistics:
  Rcvd: 0 input, 0 checksum errors, 0 length errors
        0 no port, 0 dropped
  Sent: 0 output

TCP statistics:
  Rcvd: 0 input, 0 checksum errors
  Sent: 0 output, 0 retransmitted
```

Related Commands

Command	Description
show ipv6 traffic	Displays IPv6 traffic statistics.

clear mls cef ipv6 accounting per-prefix

To clear information about the IPv6 per-prefix accounting statistics, use the **clear mls cef ipv6 accounting per-prefix** command in privileged EXEC mode.

clear mls cef ipv6 accounting per-prefix {**all** | *ipv6-address*/*mask* [*instance*]}

Syntax Description

all	Clears all per-prefix accounting statistics information.
ipv6-address/*mask*	Entry IPv6 address and mask. The format used is X:X:X:X::X/*mask,* where the valid values for *mask* are from 0 to 128.
instance	(Optional) VPN routing and forwarding instance name.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(17a)SX	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 12.2(33)SRA.

Usage Guidelines

When entering the *ipv6-address*/*mask* arguments, use this format, X:X:X:X::X/*mask,* where the valid values for *mask* are from 0 to 128.

Examples

This example shows how to clear all information about the per-prefix accounting statistics:

```
Router# clear mls cef ipv6 accounting per-prefix all
```

clear ospfv3 counters

To clear Open Shortest Path First version 3 (OSPFv3) counters, use the **clear ospfv3 counters** command in privileged EXEC mode.

clear ospfv3 [*process-id*] [*address-family*] **counters** [**neighbor** [*neighbor-interface* | *neighbor-id*]]

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
neighbor	(Optional) Neighbor statistics per interface or neighbor ID.
neighbor-interface	(Optional) Specified neighbor interface.
neighbor-id	(Optional) IPv6 or IPv4 address of the neighbor.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

Use the **neighbor** *neighbor-interface* option to clear counters for all neighbors on a specified interface. If the **neighbor** *neighbor-interface* option is not used, all OSPFv3 counters are cleared.

Examples

The following example clears all neighbors on the serial 19/0 interface:

```
Router# clear ospfv3 counters neighbor s19/0
```

clear ospfv3 force-spf

To run shortest path first (SPF) calculations for an Open Shortest Path First version 3 (OSPFv3) process, use the **clear ospfv3 counters** command in privileged EXEC mode.

clear ospfv3 [*process-id*] [*address-family*] **force-spf**

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

Use the **clear ospv3 force-spf** command to run SPF calculations for either an IPv6 or an IPv4 OSPFv3 instance. If the optional *process-ID* argument is not used, SPF runs on all instances on the interface.

Examples

The following example enables SPF calculations for process 1:

```
Router# clear ospfv3 1 force-spf
```

clear ospfv3 process

To reset an Open Shortest Path First version 3 (OSPFv3) process, use the **clear ospfv3 process** command in privileged EXEC mode.

clear ospfv3 [*process-id*] [*address-family*] **process**

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

Use the **clear ospv3 process** command to reset either an IPv6 or IPv4 OSPFv3 process. If the optional *process-ID* argument is not used, all OSPFv3 processes are reset.

Examples

The following example resets the OSPFv3 process 2:

```
Router# clear ospfv3 2 process
```

clear ospfv3 redistribution

To clear Open Shortest Path First version 3 (OSPFv3) route redistribution, use the **clear ospfv3 process** command in privileged EXEC mode.

clear ospfv3 [*process-id*] [*address-family*] **redistribution**

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

Use the **clear ospv3 process** command to clear either IPv6 or IPv4 OSPFv3 redistribution. If the optional *process-ID* argument is not used, all processes on the interface are cleared.

Examples

The following example clears OSPFv3 redistribution on all OSPFv3 processes:

```
Router# clear ospfv3 redistribution
```

clear ospfv3 traffic

To reset counters and clear Open Shortest Path First version 3 (OSPFv3) traffic statistics, use the **clear ospfv3 traffic** command privileged EXEC mode.

clear ospfv3 [*process-id*] [*address-family*] **traffic** [*interface*]

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
interface	(Optional) Specified interface from which to clear traffic statistics.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

Use the **clear ospv3 traffic** command to reset traffic statistics for an IPv6 or IPv4 OSPFv3 process. If the optional *process-ID* argument is not used, all traffic statistics are cleared.

Examples

The following example resets the counters and clears the OSPFv3 traffics statistics:

```
Router# clear ospfv3 traffic
```

codec (DSP farm profile)

To specify the codecs that are supported by a digital signal processor (DSP) farm profile, use the **codec** command in DSP farm profile configuration mode. To remove the codec, use the **no** form of this command.

codec {*codec-type* [*resolution*] | [**frame-rate** *framerate*] | [**bitrate** *bitrate*] | [**rfc-2190**] | **pass-through**}

no codec {*codec-type* [*resolution*] | [**frame-rate** *framerate*] | [**bitrate** *bitrate*] | [**rfc-2190**] | **pass-through**}

Syntax Description

codec-type	Specifies the codec preferred. • **g711alaw**—G.711 a-law 64,000 bits per second (bps) • **g711ulaw**—G.711 mu-law 64,000 bps • **g722r-64**—G.722-64 at 64,000 bps • **g729abr8**—G.729 ANNEX A and B 8000 bps • **g729ar8**—G.729 ANNEX A 8000 bps • **g729br8**—G.729 ANNEX B 8000 bps • **g729r8**—G.729 8000 bps • **h263**—H.263 video codec • **h264**—H.264 video codec • **ilbc**—Internet Low Bitrate Codec (iLBC) • **isac**—Cisco internet Speech Audio Codec (iSAC) codec
resolution	Specifies the supported video resolution. The valid entries are: • For H.263—**qcif** and **cif** • For H.264—**qcif**, **cif**, **vga**, **w360p**, **w448p**, **4cif**, and **720p** **Note** 720p option applies only to homogeneous video conferences.
frame-rate *framerate*	Specifies the frame rate. The valid entries are 15 fps or 30 fps. This option applies to homogeneous conferences only.
bitrate *bitrate*	Specifies the bitrate. This option applies to homogeneous conferences only.
rfc-2190	Specifies the payload format follow RFC-2190.
pass-through	Enables codec pass-through. Supported for transcoding and media termination point (MTP) profiles.

Command Default

The following transcoding defaults apply when you are configuring audio profiles only. When you configure video transcoding, you must specify the audio codecs.

Transcoding

- **g711alaw**

- **g711ulaw**
- **g729abr8**
- **g729ar8**

Conferencing

- **g711alaw**
- **g711ulaw**
- **g729abr8**
- **g729ar8**
- **g729br8**
- **g729r8**

MTP

- **g711ulaw**

Command Modes

DSP farm profile configuration (config-dspfarm-profile)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4(4)T	The **pass-through** keyword was added.
12.4(11)XJ2	The **gsmefr** and **gsmfr** keywords were removed as configurable codec options for all platforms.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.
12.4(15)XY	The **g722r-64** keyword was added.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.4(22)T	Support for IPv6 was added.
15.1(1))T	This command was modified. The **isac** keyword was added.
15.1(4)M	This command was modified. The **frame-rate**, **bitrate**, **rfc-2190**, and **pass-through** keywords were added and codec support was added for **ilbc**, **h.263** and **h.264**.

Usage Guidelines

Only one codec is supported for each MTP profile. To support multiple codecs, you must define a separate MTP profile for each codec.

For homogeneous video profiles, only one video format is supported

For heterogeneous and heterogeneous guaranteed-audio video profiles, multiple video formats and audio codecs are supported.

To change the configured codec in the profile, you must first enter a **no maximum session** command.

Table 8 shows the relationship between DSP farm functions and codecs.

Table 8 DSP Farm Functions and Codec Relationships

DSP Farm Function	Supported Codec
Transcoding	• **g711alaw** • **g711ulaw** • **g729abr8** • **g729ar8** • **iSAC** • **h263** • **h264**
Conferencing	• **g711alaw** • **g711ulaw** • **g722r-64** • **g729abr8** • **g729ar8** • **g729br8** • **g729r8** • **h263** • **h264** • **ilbc**
MTP	• **g711ulaw** • **iSAC**

Hardware MTPs support only G.711 a-law and G.711 mu-law. If you configure a profile as a hardware MTP and you want to change the codec to other than G.711, you must first remove the hardware MTP by using the **no maximum sessions hardware** command.

The **pass-through** keyword is supported for transcoding and MTP profiles only; the keyword is not supported for conferencing profiles. To support the Resource Reservation Protocol (RSVP) agent on a Skinny Client Control Protocol (SCCP) device, you must use the **codec pass-through** command. In the pass-through mode, the SCCP device processes the media stream by using a pure software MTP, regardless of the nature of the stream, which enables video and data streams to be processed in addition to audio streams. When the pass-through mode is set in a transcoding profile, no transcoding is done for the session; the transcoding device performs a pure software MTP function. The pass-through mode can be used for secure Real-Time Transport Protocol (RTP) sessions.

Examples

The following example shows how to set the call density and codec complexity to g729abr8:

```
Router(config)# dspfarm profile 123 transcode
Router(config-dspfarm-profile)# codec g729abr8
```

The following example shows how to set up a video conference with guaranteed-audio.

```
Router(config)# dspfarm profile 99 conference video guaranteed-audio
Router(config-dspfarm-profile)# codec h264 4cif
Router(config-dspfarm-profile)# codec h264 cif
Router(config-dspfarm-profile)# maximum conference-participants 8
```

Related Commands

Command	Description
associate application	Associates the SCCP protocol to the DSP farm profile.
dspfarm profile	Enters DSP farm profile configuration mode and defines a profile for DSP farm services.
maximum sessions (DSP Farm profile)	Specifies the maximum number of sessions that are supported by the profile.
rsvp	Enables RSVP support on a transcoding or MTP device.
maximum conference-participants (DSP Farm profile)	Specifies the maximum number of conference participants that are supported by this profile.
shutdown (DSP Farm profile)	Disables a DSP farm profile.

compatible rfc1583

To calculate the method used to calculate external route preferences per RFC 1583, use the **compatible rfc1583** command in router configuration mode. To disable RFC 1583 compatibility, use the **no** form of this command.

compatible rfc1583

no compatible rfc1583

Syntax Description

This command has no arguments or keywords.

Command Default

Compatible with RFC 1583.

Command Modes

OSPFv3 router configuration mode (config-router)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.

Usage Guidelines

RFC 2328 describes a new method of calculating path preferences for AS external routes:

- Intra-area paths using non-backbone areas are always the most preferred.
- The other paths—intra-area backbone paths and inter-area paths—are of equal preference.

Use the **no compatible rfc1583** command to enable the calculation method used per RFC 2328. For more detailed information, see the "RFC 1583 Compatibility" section in RFC 2328.

Caution To minimize the chance of routing loops, all Open Shortest Path First (OSPF) routers in an OSPF routing domain should have RFC compatibility set identically.

Examples

The following example specifies that the router process is compatible with RFC 1583:

```
router ospf 1
 compatible rfc1583
 !
```

context

Note Effective with Cisco IOS Release 15.0(1)M, the **context** command is replaced by the **snmp context** command. See the **snmp context** command for more information.

To associate a Simple Network Management Protocol (SNMP) context with a particular VPN routing and forwarding (VRF) instance, use the **context** command in VRF configuration mode. To disassociate an SNMP context from a VPN, use the **no** form of this command.

context *context-name*

no context

Syntax Description

context-name	Name of the SNMP VPN context. The name can be up to 32 alphanumeric characters.

Command Default

No SNMP contexts are associated with VPNs.

Command Modes

VRF configuration (config-vrf)

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)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 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	This command was modified. 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.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
15.0(1)M	This command was replaced by the **snmp context** command.

Usage Guidelines

Before you use the **context** command to associate an SNMP context with a VPN, you must do the following:

- Issue the **snmp-server context** command to create an SNMP context.
- Associate a VPN with a context so that the specific MIB data for that VPN exists in the context.
- Associate a VPN group with the context of the VPN using the **context** *context-name* keyword argument pair of the **snmp-server group** command.

SNMP contexts provide VPN users with a secure way of accessing MIB data. When a VPN is associated with a context, MIB data for that VPN exists in that context. Associating a VPN with a context helps service providers to manage networks with multiple VPNs. Creating and associating a context with a VPN enables a provider to prevent the users of one VPN from accessing information about other VPN users on the same networking device.

A route distinguisher (RD) is required to configure an SNMP context. An RD creates routing and forwarding tables and specifies the default route distinguisher for a VPN. The RD is added to the beginning of an IPv4 prefix to make it globally unique. An RD is either an autonomous system number (ASN) relative, which means that it is composed of an autonomous system number and an arbitrary number, or an IP address relative and is composed of an IP address and an arbitrary number.

Examples

The following example shows how to create an SNMP context named context1 and associate the context with the VRF named vrf1:

```
Router(config)# snmp-server context context1
Router(config)# ip vrf vrf1
Router(config-vrf)# rd 100:120
Router(config-vrf)# context context1
```

Related Commands

Command	Description
ip vrf	Enters VRF configuration mode for the configuration of a VRF.
snmp mib community-map	Associates an SNMP community with an SNMP context, engine ID, or security name.
snmp mib target list	Creates a list of target VRFs and hosts to associate with an SNMP v1 or v2c community.
snmp-server context	Creates an SNMP context.
snmp-server group	Configures a new SNMP group or a table that maps SNMP users to SNMP views.
snmp-server trap authentication vrf	Controls VRF-specific SNMP authentication failure notifications.
snmp-server user	Configures a new user to an SNMP group.

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.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

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 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 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.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

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 CommandsI

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 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.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

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 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 9 for sample times) and takes longer to use.

Table 9 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 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 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 9876543210987654987654321098765 4
 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 9876543210987654987654321098765 4
 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 (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 (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 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 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 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.

ctunnel mode

To transport IPv4 and IPv6 packets over Connectionless Network Service (CLNS) tunnel (CTunnel), use the **ctunnel mode** command in interface configuration mode. To return the ctunnel to the default **cisco** mode, use the **no** form of this command.

ctunnel mode [**gre** | **cisco**]

no ctunnel mode

Syntax Description

gre	(Optional) Sets the ctunnel mode to Generic Routing Encapsulation (GRE) for transporting IPv6 packets over the CLNS network.
cisco	(Optional) Returns the ctunnel mode to the default cisco.

Command Default

Cisco encapsulation tunnel mode is the default.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)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.

Usage Guidelines

GRE tunneling of IPv4 and IPv6 packets through CLNS-only networks enables Cisco ctunnels to interoperate with networking equipment from other vendors. This feature provides compliance with RFC 3147, *Generic Routing Encapsulation over CLNS Networks*, which should allow interoperation between Cisco equipment and that of other vendors. in which the same standard is implemented.

RFC 3147 specifies the use of GRE when tunneling packets. The implementation of this feature does not include support for GRE header fields such as those used to specify checksums, keys, or sequencing. Any packets received which specify the use of these features will be dropped.

The default ctunnel mode continues to use the standard Cisco encapsulation. Both ends of the tunnel must be configured with the same mode for it to work. If you want to tunnel ipv6 packets you must use the new gre mode.

Examples

The following example configures a CTunnel from one router to another and shows the CTunnel destination set to 49.0001.1111.1111.1111.00. The ctunnel mode is set to gre to transport IPv6 packets.

```
interface ctunnel 301
 ipv6 address 2001:0DB8:1111:2222::2/64
 ctunnel destination 49.0001.1111.1111.1111.00
```

```
ctunnel mode gre
```

Related Commands

Command	Description
clns routing	Enables routing of CLNS packets.
ctunnel destination	Specifies the destination for the CTunnel.
debug ctunnel	Displays debug messages for the IP over a CLNS Tunnel feature.
interface ctunnel	Creates a virtual interface to transport IP over a CLNS tunnel.
ip address	Sets a primary or secondary IP address for an interface.

debug adjacency

To enable the display of information about the adjacency database, use the **debug adjacency** command in privileged EXEC mode. To disable the display of these events, use the **no** form of this command.

debug adjacency [**epoch** | **ipc** | **state** | **table**] [*prefix*] [*interface*] [**connectionid** *id*] [**link** {**ipv4** | **ipv6** | **mpls**}]

no debug adjacency [**epoch** | **ipc** | **state** | **table**] [*prefix*] [*interface*] [**connectionid** *id*] [**link** {**ipv4** | **ipv6** | **mpls**}]

Syntax Description

epoch	(Optional) Displays adjacency epoch events.
ipc	(Optional) Displays interprocess communication (IPC) events for adjacencies.
state	(Optional) Displays adjacency system state machine events.
table	(Optional) Displays adjacency table operations.
prefix	(Optional) Displays debugging events for the specified IP address or IPv6 address. **Note** On the Cisco 10000 series routers, IPv6 is supported in Cisco IOS Release 12.2(28)SB and later releases.
interface	(Optional) Displays debugging events for the specified interface. For line cards, you must specify the line card if_number (interface number). Use the **show cef interface** command to obtain line card if_numbers.
connectionid *id*	(Optional) Displays debugging events for the specified client connection identification number.
link {**ipv4** | **ipv6** | **mpls**}	(Optional) Displays debugging events for the specified link type (IP, IPv6, or Multiprotocol Label Switching [MPLS] traffic). **Note** On the Cisco 10000 series routers, IPv6 is supported in Cisco IOS Release 12.2(28)SB and later releases.

Command Default

Debugging events are not displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(7)XE	This command was introduced on the Cisco 7600 series routers.
12.1(1)E	This command was implemented on the Cisco 7600 series routers.
12.2(14)SX	This command was implemented on the Supervisor Engine 720.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S, and the *prefix*, *interface*, **connectionid** *id*, and **link** {**ipv4** | **ipv6** | **mpls**} keywords and arguments were added.

Release	Modification
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, you should use debug commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Also, you should use debug commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased debug command processing overhead will affect system use.

You can use any combination of the *prefix*, *interface*, **connectionid** *id*, and **link** {**ipv4 | ipv6 | mpls**} keywords and arguments (in any order) as a filter to enable debugging for a specified subset of adjacencies.

Note On the Cisco 10000 series routers, IPv6 is supported in Cisco IOS Release 12.2(28)SB and later releases.

Examples

The following example shows how to display information on the adjacency database:

```
Router# debug adjacency

*Jan 27 06:22:50.543: ADJ-ios_mgr: repopulate adjs on up event for Ethernet3/0
*Jan 27 06:22:50.543: ADJ: IPV6 adj out of Ethernet3/0, addr FE80::20C:CFFF:FEDF:6854
(incomplete) no src set: init/update from interface
*Jan 27 06:22:50.543: ADJ: IPV6 adj out of Ethernet3/0, addr FE80::20C:CFFF:FEDF:6854
(incomplete) no src set: set bundle to IPv6 adjacency oce
*Jan 27 06:22:50.543: ADJ: IPV6 adj out of Ethernet3/0, addr FE80::20C:CFFF:FEDF:6854
(incomplete) no src set: allocated, setup and inserted OK
*Jan 27 06:22:50.543: ADJ: IPV6 adj out of Ethernet3/0, addr FE80::20C:CFFF:FEDF:6854
(incomplete) src IPv6 ND: source IPv6 ND added OK
*Jan 27 06:22:50.543: ADJ: IPV6 adj out of Ethernet3/0, addr FE80::20C:CFFF:FEDF:6854
(incomplete) src IPv6 ND: computed macstring (len 14): OK
*Jan 27 06:22:50.543: ADJ: IPV6 adj out of Ethernet3/0, addr FE80::20C:CFFF:FEDF:6854 src
IPv6 ND: made complete (macstring len 0 to 14/0 octets)
00:04:40: %LINK-3-UPDOWN: Interface Ethernet3/0, changed state to up
00:04:41: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet3/0, changed
```

Related Commands

Command	Description
clear adjacency	Clears the Cisco Express Forwarding adjacency table.
clear arp-cache	Deletes all dynamic entries from the ARP cache.
show adjacency	Displays Cisco Express Forwarding adjacency table information.
show mls cef adjacency	Displays information about the hardware Layer 3 switching adjacency node.

debug bfd

To display debugging messages about Bidirectional Forwarding Detection (BFD), use the **debug bfd** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

Cisco IOS Release 12.2(18)SXE, 12.4(4)T, and 12.2(33)SRA

debug bfd {**event** | **packet** [*ip-address* | *ipv6-address*]}

no debug bfd {**event** | **packet** [*ip-address* | *ipv6-address*]}

Cisco IOS Release 12.0(31)S

debug bfd {**event** | **packet** [*ip-address*] | **ipc-error** | **ipc-event** | **oir-error** | **oir-event**}

no debug bfd {**event** | **packet** [*ip-address*] | **ipc-error** | **ipc-event** | **oir-error** | **oir-event**}

Syntax Description

event	Displays debugging information about BFD state transitions.
packet	Displays debugging information about BFD control packets.
ip-address	(Optional) Displays debugging information about BFD only for the specified IP address.
ipv6-address	(Optional) Displays debugging information about BFD only for the specified IPv6 address.
ipc-error	(Optional) Displays debugging information with interprocess communication (IPC) errors on the Route Processor (RP) and line card (LC).
ipc-event	(Optional) Displays debugging information with IPC events on the RP and LC.
oir-error	(Optional) Displays debugging information with online insertion and removal (OIR) errors on the RP and LC.
oir-event	(Optional) Displays debugging information with OIR events on the RP and LC.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXE	This command was introduced.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S.
12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRE	This command was modified. Support for IPv6 was added.
15.1(2)T	This command was modified. Support for IPv6 was added to Cisco IOS Release 15.1(2)T.

Usage Guidelines

The **debug bfd** command can be used to troubleshoot the BFD feature.

Note Because BFD is designed to send and receive packets at a very high rate of speed, consider the potential effect on system resources before enabling this command, especially if there are a large number of BFD peers. The **debug bfd packet** command should be enabled only on a live network at the direction of Cisco Technical Assistance Center personnel.

Examples

The following example shows output from the **debug bfd packet** command. The IP address has been specified in order to limit the packet information to one interface:

```
Router# debug bfd packet 172.16.10.5

BFD packet debugging is on
*Jan 26 14:47:37.645: Tx*IP: dst 172.16.10.1, plen 24. BFD: diag 2, St/D/P/F (1/0/0/0),
mult 5, len 24, loc/rem discr 1 1, tx 1000000, rx 1000000 100000, timer 1000 ms, #103
*Jan 26 14:47:37.645: %OSPF-5-ADJCHG: Process 10, Nbr 172.16.10.12 on Ethernet1/4 from
FULL to DOWN, Neighbor Down: BFD node down
*Jan 26 14:47:50.685: %OSPF-5-ADJCHG: Process 10, Nbr 172.16.10.12 on Ethernet1/4 from
LOADING to FULL, Loading Done
*Jan 26 14:48:00.905: Rx  IP: src 172.16.10.1, plen 24. BFD: diag 0, St/D/P/F (1/0/0/0),
mult 4, len 24, loc/rem discr 2 1, tx 1000000, rx 1000000 100000, timer 4000 ms, #50
*Jan 26 14:48:00.905: Tx IP: dst 172.16.10.1, plen 24. BFD: diag 2, St/D/P/F (2/0/0/0),
mult 5, len 24, loc/rem discr 1 2, tx 1000000, rx 1000000 100000, timer 1000 ms, #131
*Jan 26 14:48:00.905: Rx  IP: src 172.16.10.1, plen 24. BFD: diag 0, St/D/P/F (3/0/0/0),
mult 4, len 24, loc/rem discr 2 1, tx 1000000, rx 1000000 100000, timer 4000 ms, #51
*Jan 26 14:48:00.905: Tx IP: dst 172.16.10.1, plen 24. BFD: diag 0, St/D/P/F (3/0/0/0),
mult 5, len 24, loc/rem discr 1 2, tx 1000000, rx 1000000 100000, timer 1000 ms, #132
```

The following example shows output from the **debug bfd event** command when an interface between two BFD neighbor routers fails and then comes back online:

```
Router# debug bfd event

22:53:48: BFD: bfd_neighbor - action:DESTROY, proc:1024, idb:FastEthernet0/1,
neighbor:172.16.10.2
22:53:48: BFD: bfd_neighbor - action:DESTROY, proc:512, idb:FastEthernet0/1,
neighbor:172.16.10.2
22:53:49: Session [172.16.10.1,172.16.10.2,Fa0/1,1], event DETECT TIMER EXPIRED, state UP
-> FAILING
.
.
.
22:56:35: BFD: bfd_neighbor - action:CREATE, proc:1024, idb:FastEthernet0/1,
neighbor:172.16.10.2
22:56:37: Session [172.16.10.1,172.16.10.2,Fa0/1,1], event RX IHY 0, state FAILING -> DOWN
22:56:37: Session [172.16.10.1,172.16.10.2,Fa0/1,1], event RX IHY 0, state DOWN -> INIT
22:56:37: Session [172.16.10.1,172.16.10.2,Fa0/1,1], event RX IHY 1, state INIT -> UP
```

Table 10 describes the significant fields shown in the display.

Table 10 debug bfd event Field Descriptions

Field	Description
bfd_neighbor - action:DESTROY	The BFD neighbor will tear down the BFD session.
Session [172.16.10.1, 172.16.10.2, Fa0/1,1]	IP addresses of the BFD neighbors holding this session that is carried over FastEthernet interface 0/1.
event DETECT TIMER EXPIRED	The BFD neighbor has not received BFD control packets within the negotiated interval and the detect timer has expired.
state UP -> FAILING	The BFD event state is changing from Up to Failing.
Session [172.16.10.1, 172.16.10.2, Fa0/1,1], event RX IHY 0	The BFD session between the neighbors indicated by the IP addresses that is carried over FastEthernet interface 0/1 is changing state from Failing to Down. The I Hear You (IHY) bit value is shown as 0 to indicate that the remote system is tearing down the BFD session.
event RX IHY 0, state DOWN -> INIT	The BFD session is still considered down, and the IHY bit value still is shown as 0, and the session state changes from DOWN to INIT to indicate that the BFD session is again initializing, as the interface comes back up.
event RX IHY 1, state INIT -> UP	The BFD session has been reestablished, and the IHY bit value changes to 1 to indicate that the session is live. The BFD session state changes from INIT to UP.

The following example shows output from the **debug bfd packet** command when an interface between two BFD neighbor routers fails and then comes back online. The diagnostic code changes from 0 (No Diagnostic) to 1 (Control Detection Time Expired) because no BFD control packets could be sent (and therefore detected by the BFD peer) after the interface fails. When the interface comes back online, the diagnostic code changes back to 0 to signify that BFD packets can be sent and received by the BFD peers.

```
Router# debug bfd packet

23:03:25: Rx  IP: src 172.16.10.2, plen 24. BFD: diag 0, H/D/P/F (0/0/0/0), mult 3, len
24, loc/rem discr 5 1, tx 1000000, rx 100007
23:03:25: Tx IP: dst 172.16.10.2, plen 24. BFD: diag 1, H/D/P/F (0/0/0/0), mult 5, len 24,
loc/rem discr 1 5, tx 1000000, rx 1000008
23:03:25: Tx IP: dst 172.16.10.2, plen 24. BFD: diag 1, H/D/P/F (1/0/0/0), mult 5, len 24,
loc/rem discr 1 5, tx 1000000, rx 1000009
```

Table 11 describes the significant fields shown in the display.

Table 11 debug bfd packet Field Descriptions

Field	Description
Rx IP: src 172.16.10.2	The router has received this BFD packet from the BFD router with source address 172.16.10.2.
plen 24	Length of the BFD control packet, in bytes.

Table 11 debug bfd packet Field Descriptions (continued)

Field	Description
diag 0	A diagnostic code specifying the local system's reason for the last transition of the session from Up to some other state. State values are as follows: • 0—No Diagnostic • 1—Control Detection Time Expired • 2—Echo Function Failed • 3—Neighbor Signaled Session Down • 4—Forwarding Plane Reset • 5—Path Down • 6—Concentrated Path Down • 7—Administratively Down
H/D/P/F (0/0/0/0)	H bit—Hear You bit. This bit is set to 0 if the transmitting system either is not receiving BFD packets from the remote system or is tearing down the BFD session. During normal operation the I Hear You bit is set to 1. D bit—Demand Mode bit. If the Demand Mode bit set, the transmitting system wants to operate in demand mode. BFS has two modes—asynchronous and demand. The Cisco implementation of BFD supports only asynchronous mode. P bit—Poll bit. If the Poll bit is set, the transmitting system is requesting verification of connectivity or of a parameter change. F bit—Final bit. If the Final bit is set, the transmitting system is responding to a received BFC control packet that had a Poll (P) bit set.
mult 3	Detect time multiplier. The negotiated transmit interval, multiplied by the detect time multiplier, determines the detection time for the transmitting system in BFD asynchronous mode. The detect time multiplier is similar to the hello multiplier in IS-IS, which is used to determine the hold timer: (hellointerval) * (hellomultiplier) = hold timer. If a hello packet is not received within the hold-timer interval, a failure has occurred. Similarly, for BFD: (transmit interval) * (detect multiplier) = detect timer. If a BFD control packet is not received from the remote system within the detect-timer interval, a failure has occurred.
len 24	The BFD packet length.

Table 11 debug bfd packet Field Descriptions (continued)

Field	Description
loc/rem discr 5 1	The values for My Discriminator (local) and Your Discriminator (remote) BFD neighbors. • My Discriminator—Unique, nonzero discriminator value generated by the transmitting system, used to demultiplex multiple BFD sessions between the same pair of systems. • Your Discriminator—The discriminator received from the corresponding remote system. This field reflects the received value of My Discriminator, or is zero if that value is unknown.
tx 1000000	Desired minimum transmit interval.
rx 100007	Required minimum receive interval.

debug bgp ipv6 dampening

To display debugging messages for IPv6 Border Gateway Protocol (BGP) dampening, use the **debug bgp ipv6 dampening** command in privileged EXEC mode. To disable debugging messages for IPv6 BGP dampening, use the **no** form of this command.

debug bgp ipv6 {**unicast** | **multicast**} **dampening** [**prefix-list** *prefix-list-name*]

no debug bgp ipv6 {**unicast** | **multicast**} **dampening** [**prefix-list** *prefix-list-name*]

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.
prefix-list *prefix-list-name*	(Optional) Name of an IPv6 prefix list.

Command Default

Debugging for IPv6 BGP dampening packets is not enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)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(13)T	The **prefix-list** keyword was added.
12.0(24)S	The **prefix-list** keyword was added.
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.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
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 introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The **debug bgp ipv6 dampening** command is similar to the **debug ip bgp dampening** command, except that it is IPv6-specific.

Use the **prefix-list** keyword and an argument to filter BGP IPv6 dampening debug information through an IPv6 prefix list.

Note By default, the network server sends the output from debug commands and system error messages to the console. To redirect debugging output, use the **logging** command options within global configuration mode. Destinations are the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server.

Examples

The following is sample output from the **debug bgp ipv6 dampening** command:

```
Router# debug bgp ipv6 dampening

00:13:28:BGP(1):charge penalty for 2000:0:0:1::/64 path 2 1 with halflife-time 15
reuse/suppress 750/2000
00:13:28:BGP(1):flapped 1 times since 00:00:00. New penalty is 1000
00:13:28:BGP(1):charge penalty for 2000:0:0:1:1::/80 path 2 1 with halflife-time 15
reuse/suppress 750/2000
00:13:28:BGP(1):flapped 1 times since 00:00:00. New penalty is 1000
00:13:28:BGP(1):charge penalty for 2000:0:0:5::/64 path 2 1 with halflife-time 15
reuse/suppress 750/2000
00:13:28:BGP(1):flapped 1 times since 00:00:00. New penalty is 1000
00:16:03:BGP(1):charge penalty for 2000:0:0:1::/64 path 2 1 with halflife-time 15
reuse/suppress 750/2000
00:16:03:BGP(1):flapped 2 times since 00:02:35. New penalty is 1892

00:18:28:BGP(1):suppress 2000:0:0:1:1::/80 path 2 1 for 00:27:30 (penalty 2671)
00:18:28:halflife-time 15, reuse/suppress 750/2000
00:18:28:BGP(1):suppress 2000:0:0:1::/64 path 2 1 for 00:27:20 (penalty 2664)
00:18:28:halflife-time 15, reuse/suppress 750/2000
```

The following example shows output for the **debug bgp ipv6 dampening** command filtered through the prefix list named marketing:

```
Router# debug bgp ipv6 dampening prefix-list marketing

00:16:08:BGP(1):charge penalty for 2001:0DB8::/64 path 30 with halflife-time 15
reuse/suppress 750/2000
00:16:08:BGP(1):flapped 1 times since 00:00:00. New penalty is 10
```

Table 12 describes the fields shown in the display.

Table 12 debug bgp ipv6 dampening Field Descriptions

Field	Description
penalty	Numerical value of 1000 assigned to a route by a router configured for route dampening in another autonomous system each time a route flaps. Penalties are cumulative. The penalty for the route is stored in the BGP routing table until the penalty exceeds the suppress limit. If the penalty exceeds the suppress limit, the route state changes from history to damp.
flapped	Number of times a route is available, then unavailable, or vice versa.
halflife-time	Amount of time (in minutes) by which the penalty is decreased after the route is assigned a penalty. The halflife-time value is half of the half-life period (which is 15 minutes by default). Penalty reduction happens every 5 seconds.

Table 12 debug bgp ipv6 dampening Field Descriptions (continued)

Field	Description
reuse	The limit by which a route is unsuppressed. If the penalty for a flapping route decreases and falls below this reuse limit, the route is unsuppressed. That is, the route is added back to the BGP table and once again used for forwarding. The default reuse limit is 750. Routes are unsuppressed at 10-second increments. Every 10 seconds, the router determines which routes are now unsuppressed and advertises them to the world.
suppress	Limit by which a route is suppressed. If the penalty exceeds this limit, the route is suppressed. The default value is 2000.
maximum suppress limit (not shown in sample output)	Maximum amount of time (in minutes) a route is suppressed. The default value is four times the half-life period.
damp state (not shown in sample output)	State in which the route has flapped so often that the router will not advertise this route to BGP neighbors.

Related Commands

Command	Description
debug bgp ipv6 updates	Displays debugging messages for IPv6 BGP update packets.

debug bgp ipv6 updates

To display debugging messages for IPv6 Border Gateway Protocol (BGP) update packets, use the **debug bgp ipv6 updates** command in privileged EXEC mode. To disable debugging messages for IPv6 BGP update packets, use the **no** form of this command.

debug bgp ipv6 {**unicast** | **multicast**} **updates** [*ipv6-address*] [**prefix-list** *prefix-list-name*] [**in** | **out**]

no debug bgp ipv6 {**unicast** | **multicast**} **updates** [*ipv6-address*] [**prefix-list** *prefix-list-name*] [**in** | **out**]

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.
ipv6-address	(Optional) The IPv6 address of a BGP neighbor. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
prefix-list *prefix-list-name*	(Optional) Name of an IPv6 prefix list.
in	(Optional) Indicates inbound updates.
out	(Optional) Indicates outbound updates.

Command Default

Debugging for IPv6 BGP update packets is not enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)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(13)T	The **prefix-list** keyword was added.
12.0(24)S	The **prefix-list** keyword was added.
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.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
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 introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The **debug bgp ipv6 updates** command is similar to the **debug ip bgp updates** command, except that it is IPv6-specific.

Use the **prefix-list** keyword to filter BGP IPv6 updates debugging information through an IPv6 prefix list.

Note By default, the network server sends the output from **debug** commands and system error messages to the console. To redirect debugging output, use the **logging** command options within global configuration mode. Destinations are the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server. For complete information on **debug** commands and redirecting debugging output, refer to the Release 12.2 *Cisco IOS Debug Command Reference*.

Examples

The following is sample output from the **debug bgp ipv6 updates** command:

```
Router# debug bgp ipv6 updates

14:04:17:BGP(1):2000:0:0:2::2 computing updates, afi 1, neighbor version 0, table version
1, starting at ::
14:04:17:BGP(1):2000:0:0:2::2 update run completed, afi 1, ran for 0ms, neighbor version
0, start version 1, throttled to 1
14:04:19:BGP(1):sourced route for 2000:0:0:2::1/64 path #0 changed (weight 32768)
14:04:19:BGP(1):2000:0:0:2::1/64 route sourced locally
14:04:19:BGP(1):2000:0:0:2:1::/80 route sourced locally
14:04:19:BGP(1):2000:0:0:3::2/64 route sourced locally
14:04:19:BGP(1):2000:0:0:4::2/64 route sourced locally
14:04:22:BGP(1):2000:0:0:2::2 computing updates, afi 1, neighbor version 1, table version
6, starting at ::
14:04:22:BGP(1):2000:0:0:2::2 send UPDATE (format) 2000:0:0:2::1/64, next 2000:0:0:2::1,
metric 0, path
14:04:22:BGP(1):2000:0:0:2::2 send UPDATE (format) 2000:0:0:2:1::/80, next 2000:0:0:2::1,
metric 0, path
14:04:22:BGP(1):2000:0:0:2::2 send UPDATE (prepend, chgflags:0x208) 2000:0:0:3::2/64, next
2000:0:0:2::1, metric 0, path
14:04:22:BGP(1):2000:0:0:2::2 send UPDATE (prepend, chgflags:0x208) 2000:0:0:4::2/64, next
2000:0:0:2::1, metric 0, path
```

The following is sample output from the **debug bgp ipv6 updates** command filtered through the prefix list named sales:

```
Router# debug bgp ipv6 updates prefix-list sales

00:18:26:BGP(1):2000:8493:1::2 send UPDATE (prepend, chgflags:0x208) 7878:7878::/64, next
2001:0DB8::36C, metric 0, path
```

Table 13 describes the significant fields shown in the display.

Table 13 debug bgp ipv6 updates Field Descriptions

Field	Description
BGP(1):	BGP debugging for address family index (afi) 1.
afi	Address family index.
neighbor version	Version of the BGP table on the neighbor from which the update was received.

Table 13 debug bgp ipv6 updates Field Descriptions (continued)

Field	Description
table version	Version of the BGP table on the router from which you entered the **debug bgp ipv6 updates** command.
starting at	Starting at the network layer reachability information (NLRI). BGP sends routing update messages containing NLRI to describe a route and how to get there. In this context, an NLRI is a prefix. A BGP update message carries one or more NLRI prefixes and the attributes of a route for the NLRI prefixes; the route attributes include a BGP next hop gateway address, community values, and other information.
route sourced locally	Indicates that a route is sourced locally and that updates are not sent for the route.
send UPDATE (format)	Indicates that an update message for a reachable network should be formatted. Addresses include prefix and next hop.
send UPDATE (prepend, chgflags:0x208)	Indicates that an update message about a path to a BGP peer should be written.

Related Commands

Command	Description
debug bgp ipv6 dampening	Displays debugging messages for IPv6 BGP dampening packets.

debug bgp vpnv6 unicast

To display Border Gateway Protocol (BGP) virtual private network (VPN) debugging output, use the **debug bgp vpnv6 unicast** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug bgp vpnv6 unicast

no debug bgp vpnv6

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)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.

Usage Guidelines

Use the **debug bgp vpnv6 unicast** command to help troubleshoot the BGP VPN.

Note By default, the network server sends the output from debug commands and system error messages to the console. To redirect debugging output, use the logging command options within global configuration mode. Destinations are the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server. For complete information on debug commands and redirecting debugging output, refer to the *Cisco IOS Debug Command Reference*, Release 12.4.

Examples

The following example enables BGP debugging output for IPv6 VPN instances:

```
Router# debug bgp vpnv6 unicast
```

debug crypto condition

To define conditional debug filters, use the **debug crypto condition** command in privileged EXEC mode. To disable conditional debugging, use the **no** form of this command.

debug crypto condition [**connid** *integer* **engine-id** *integer*] [**flowid** *integer* **engine-id** *integer*] [**gdoi-group** *groupname*] [**isakmp profile** *profile-name*] [**fvrf** *string*] [**ivrf** *string*] [**local** {**ipv4** *ip-address* | **ipv6** *ip-address*}] [**peer** [**group** *string*] [**hostname** *string*] [**ipv4** *ip-address* | **ipv6** *ip-address*] [**subnet** *subnet mask* | *ipv6-prefix*] [**username** *string*]] [**spi** *integer*] [**reset**] [**unmatched** [**engine**] [**gdoi-group**] [**ipsec**] [**isakmp**] [**username** *string*]]

no debug crypto condition [**connid** *integer* **engine-id** *integer*] [**flowid** *integer* **engine-id** *integer*] [**gdoi-group** *groupname*] [**isakmp profile** *profile-name*] [**fvrf** *string*] [**ivrf** *string*] [**local** {**ipv4** *ip-address* | **ipv6** *ip-address*}] [**peer** [**group** *string*] [**hostname** *string*] [**ipv4** *ip-address* | **ipv6** *ip-address*] [**subnet** *subnet mask* | *ipv6-prefix*] [**username** *string*]] [**spi** *integer*] [**reset**] [**unmatched** [**engine**] [**gdoi-group**] [**ipsec**] [**isakmp**] [**username** *string*]]

Syntax Description

connid *integer*[1]	(Optional) Specifies the Internet Key Exchange (IKE) and IP Security (IPsec) connection ID filter. Valid values range from 1 to 32766.
engine-id *integer*	(Optional) Specifies the Crypto engine ID value, which can be retrieved via the **show crypto isakmp sa detail** command. Valid values are 1, which represents software engines, and 2, which represents hardware engines.
flowid *integer*	(Optional) Specifies the IPsec flow-ID filter. Valid values range from 1 to 32766.
gdoi-group *groupname*	(Optional) Specifies the Group Domain of Interpretation (GDOI) group filter. • The *groupname* value is the name of the GDOI group.
isakmp profile *profile-name*	(Optional) Specifies the filter for the Internet Security Association Key Management Protocol (ISAKMP) profile. • The *profile-name* value is the name of the ISAKMP profile to be filtered.
fvrf *string*[1]	(Optional) Specifies the Front-door Virtual Private Network (VPN) Routing and Forwarding (FVRF) filter. The *string* argument must be the name string of an FVRF instance.
ivrf *string*[1]	(Optional) Specifies the Inside VRF (IVRF) filter. The *string* argument must be the name string of an IVRF instance.
local {**ipv4** *ip-address* | **ipv6** *ip-address*}	(Optional) Specifies the IKE local address filter. • The *ip-address* value is the IP address of the local crypto endpoint.

peer[1]	(Optional) Specifies the IKE peer filter. At least one of the following keywords and arguments must be used: • **group** *string*—Unity group name filter of the IKE peer. • **hostname** *string*—Fully qualified domain name (FQDN) hostname filter of the IKE peer. • **ipv4** *ip-address* or **ipv6** *ip-address*—IP address filter of the IKE peer. • **subnet** *subnet mask* or **subnet** *ipv6-prefix*—Range of IKE peer IP addresses or prefix length. • **username** *string*—FQDN username filter of the IKE peer.
spi *integer*[1]	(Optional) Specifies the security policy index (SPI) filter. The integer must be a 32-bit unsigned integer.
reset	(Optional) Deletes all crypto debug filters. **Note** It is suggested that you turn off all crypto global debugging before using this keyword; otherwise, your system may be flooded with debug messages.
unmatched	(Optional) Filters all debug messages or only specified debug messages by choosing any of the following keywords: • **engine**—Output crypto engine debugs even if no context is available. • **gdoi-group**—Output GDOI group debugs even if no match occurs. • **ipsec**—Output IPsec debugs even if no context is available. • **isakmp**—Output IKE debugs even if no context is available.
username *string*	(Optional) Specifies the XAUTH or PKI-AAA username filter.

1. Additional conditional filters (IP address, subnet mask, username, hostname, group, connection-ID, flow-ID, SPI, FVRF, and IVRF) can be specified more than once by repeating the **debug crypto condition** command with any of the available filters.

Defaults

Crypto conditional debugging is disabled.

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.
12.4(11)T	The **gdoi-group** *groupname*, **isakmp profile** *profile-name*, **local ipv4** *ip-address*, **unmatched**, and **username** *string* keywords and arguments were added.

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.
15.1(4)M	This command was modified. The **ipv6** keyword was added to provide support for IPv6 addresses.

Usage Guidelines

Before enabling the **debug crypto condition** command, you must decide what debug condition types (also known as debug filters) and values will be used. The volume of debug messages is dependent on the number of conditions you define.

Note Specifying numerous debug conditions may consume CPU cycles and have a negative effect on router performance.

To begin crypto conditional debugging, you must also enable at least one global crypto debug command—**debug crypto isakmp**, **debug crypto ipsec**, and **debug crypto engine**; otherwise, conditional debugging will not occur. This requirement helps to ensure that the performance of the router will not be impacted when conditional debugging is not being used.

Note Debug message filtering for hardware crypto engines is not supported.

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# no debug crypto isakmp
Router# no debug crypto ipsec
```

```
Router# no debug crypto engine
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
show crypto debug-condition	Displays crypto debug conditions that have already been enabled in the router.
show crypto debug-condition unmatched	Displays crypto conditional debug messages when context information is unavailable to check against debug conditions.
show crypto ipsec sa	Displays the settings used by current SAs.
show crypto isakmp sa	Displays all current IKE SAs at a peer.

debug crypto ipv6 ipsec

To display IP Security (IPSec) events for IPv6 networks, use the **debug crypto ipv6 ipsec** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug crypto ipv6 ipsec

no debug crypto ipv6 ipsec

Syntax Description

This command has no arguments or keywords.

Command Default

Debugging for IPv6 IPSec events is not enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

Use this command to display IPSec events while setting up or removing policy definitions during OSPF configuration.

Examples

The following example enables the display of IPSec events for IPv6 networks:

```
Router# debug crypto ipv6 ipsec
```

Related Commands

Command	Description
debug crypto engine	Displays debugging messages about crypto engines, which perform encryption and decryption.
debug crypto ipv6 packet	Displays debug messages for IPv6 packets allowing you to see the contents of packets outbound from a Cisco router when the remote node is not a Cisco node.
debug crypto socket	Displays communication between the client and IPSec during policy setup and removal processes.
debug ipv6 ospf authentication	Displays the interaction between OSPF and IPSec, including creation or removal of policies.

debug crypto ipv6 packet

To display the contents of IPv6 packets, use the **debug crypto ipv6 packet** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug crypto ipv6 packet

no debug crypto ipv6 packet

Syntax Description

This command has no arguments or keywords.

Command Default

Debugging for IPv6 IPSec packets is not enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

Consult Cisco Technical Support before using this command.

Use this command to display the contents of IPv6 packets. This command is useful when the remote node is not a Cisco device and communication between the Cisco and non-Cisco router cannot be established. This command enables you to look at the contents of the packets outbound from the Cisco router.

This command examines the content of every IPv6 packet and may slow network performance.

Examples

This example shows the output of each packet when the **debug crypto ipv6 packet** command is enabled:

```
Router# debug crypto ipv6 packet

Crypto IPv6 IPSEC packet debugging is on

Router#
*Oct 30 16:57:06.330:
IPSECv6:before Encapsulation of IPv6 packet:
0E37A7C0:                  6E000000 00285901          n....(Y.
0E37A7D0:FE800000 00000000 020A8BFF FED42C1D  ~...........~T,.
0E37A7E0:FF020000 00000000 00000000 00000005  ................
0E37A7F0:03010028 01010104 00000001 8AD80000  ...(.........X..
0E37A800:00000006 01000013 000A0028 0A0250CF  ...........(..PO
0E37A810:01010104 0A0250CF                    ......PO
*Oct 30 16:57:06.330:
IPSECv6:Encapsulated IPv6 packet
:
0E37A7B0:6E000000 00403301 FE800000 00000000  n....@3.~.......
0E37A7C0:020A8BFF FED42C1D FF020000 00000000  ....~T,.........
```

```
0E37A7D0:00000000 00000005 59040000 000022B8  ........Y....."8
0E37A7E0:0000001A 38AB1ED8 04C1C6FB FF1248CF  ....8+.X.AF{..HO
0E37A7F0:03010028 01010104 00000001 8AD80000  ...(.........X..
0E37A800:00000006 01000013 000A0028 0A0250CF  ...........(..PO
0E37A810:01010104 0A0250CF                    ......PO
*Oct 30 16:57:11.914:
IPSECv6:Before Decapsulation of IPv6 packet
:
0E004A50:                 6E000000 00403301          n....@3.
0E004A60:FE800000 00000000 023071FF FE7FE81D  ~........0q.~.h.
0E004A70:FF020000 00000000 00000000 00000005  ................
0E004A80:59040000 000022B8 00001D88 F5AC68EE  Y....."8....u,hn
0E004A90:1AC00088 947C6BF2 03010028 0A0250CF  .@...|kr...(..PO
0E004AA0:00000001 E9080000 00000004 01000013  ....i...........
0E004AB0:000A0028 0A0250CF 01010104 01010104  ...(..PO........
0E004AC0:
*Oct 30 16:57:11.914:
IPSECv6:Decapsulated IPv6 packet
:
0E004A70:6E000000 00285901 FE800000 00000000  n....(Y.~.......
0E004A80:023071FF FE7FE81D FF020000 00000000  .0q.~.h.........
0E004A90:00000000 00000005 03010028 0A0250CF  ...........(..PO
0E004AA0:00000001 E9080000 00000004 01000013  ....i...........
0E004AB0:000A0028 0A0250CF 01010104 01010104  ...(..PO........
0E004AC0:
*Oct 30 16:57:16.330:
IPSECv6:before Encapsulation of IPv6 packet:
0E003DC0:                 6E000000 00285901          n....(Y.
0E003DD0:FE800000 00000000 020A8BFF FED42C1D  ~...........~T,.
0E003DE0:FF020000 00000000 00000000 00000005  ................
0E003DF0:03010028 01010104 00000001 8AD80000  ...(.........X..
0E003E00:00000006 01000013 000A0028 0A0250CF  ...........(..PO
0E003E10:01010104 0A0250CF                    ......PO
*Oct 30 16:57:16.330:
IPSECv6:Encapsulated IPv6 packet
:
0E003DB0:6E000000 00403301 FE800000 00000000  n....@3.~.......
0E003DC0:020A8BFF FED42C1D FF020000 00000000  ....~T,.........
0E003DD0:00000000 00000005 59040000 000022B8  ........Y....."8
0E003DE0:0000001B F8E3C4E2 4CC4B690 DDF32B5C  ....xcDbLD6.]s+\
0E003DF0:03010028 01010104 00000001 8AD80000  ...(.........X..
0E003E00:00000006 01000013 000A0028 0A0250CF  ...........(..PO
0E003E10:01010104 0A0250CF                    ......PO
```

Related Commands

Command	Description
debug crypto engine	Displays debugging messages about crypto engines, which perform encryption and decryption.
debug crypto ipv6 ipsec	Displays IPSec events for IPv6 networks.
debug crypto socket	Displays communication between the client and IPSec during policy setup and removal processes.

debug dmvpn

To display debug Dynamic Multipoint VPN (DMVPN) session information, use the **debug dmvpn** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug dmvpn {**all** | **error** | **detail** | **packet**} {**all** | *debug-type*}

no debug dmvpn {**all** | **error** | **detail** | **packet**} {**all** | *debug-type*}

Syntax Description

all	Enables all levels of debugging.
error	Enables error-level debugging.
detail	Enables detail-level debugging.
packet	Enables packet-level debugging.
all	Enables NHRP, sockets, tunnel protection, and crypto debugging.
debug-type	The type of debugging that you want to enable. The following keywords can be specified for the *debug-type* argument: • **nhrp** — Enables Next Hop Resolution Protocol (NHRP) debugging only. • **crypto** — Enables crypto Internet Key Exchange (IKE) and IPsec debugging. • **tunnel** — Enables tunnel protection debugging. • **socket** — Enables crypto secure socket debugging. The keywords can be used alone, or in any combination with each other, but each keyword can be used only once.

Command Default

DMVPN debugging is disabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(9)T	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.
Cisco IOS XE Release 2.5	This command was modified. This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

You must specify both the level and the type of debugging that you want to enable. The debugging levels are all, error, detail, or packet. You can enable NHRP, crypto Internet Key Exchange (IKE) and IPsec, tunnel protection, and crypto secure socket debugging at any of the four debugging levels.

To enable conditional DMVPN debugging, you must first specify the level and type of debugging that you want to enable, and then use the **debug dmvpn condition** command to specify the conditions that you want to enable.

Error-Level Debugging

When error-level debugging is enabled with the **debug dmvpn error** command, the following debugging commands are enabled by default:

- **debug crypto ipsec error**
- **debug crypto isakmp error**
- **debug nhrp error**

Detail-Level Debugging

When detail-level debugging is enabled with the **debug dmvpn detail** command, the following debugging commands are enabled by default:

- **debug crypto ipsec**
- **debug crypto isakmp**
- **debug crypto sockets**
- **debug nhrp**
- **debug nhrp cache**
- **debug nhrp rate**
- **debug tunnel protection**

Packet-Level Debugging

When packet-level debugging is enabled with the **debug dmvpn packet** command, the following debugging commands are enabled by default:

- **debug nhrp extension**
- **debug nhrp packet**

Note Executing the **debug dmvpn all** command with a high number of active sessions may result in high CPU utilization and large data output.

NHRP Shortcut Route Debugging

When shortcut switching is enabled on the router, the system looks up the NHRP shortcut route in the Routing Information Base (RIB) in order to forward the packet to the next-hop in the DMVPN cloud.

Table 14 describes the debug messages displayed by the router when shortcut switching and NHRP debugging are both enabled.

Table 14 Sample Messages for Shortcut Switching and NHRP

Event	Sample Message
NHRP successfully adds a route to the RIB	`*Feb 21 13:11:24.043: NHRP: Adding route entry for 172.16.99.0 to RIB` `*Feb 21 13:11:24.043: NHRP: Route addition to RIB successful`
NHRP is unable to add a route to the RIB	`*Feb 21 13:11:24.043: NHRP: Adding route entry for 172.16.99.0 to RIB` `*Feb 21 13:11:24.043: NHRP: Route addition to RIB failed`
NHRP removes a route from the RIB	`*Feb 21 13:11:24.043: NHRP: Deleting route entry for 172.16.99.0 from RIB`
NHRP evicts a route from the RIB	`*Mar 1 18:24:29.371: NHRP: Route entry 172.16.22.0/24 clobbered by distance`
NHRP changes the administrative distance	`*Mar 1 00:14:16.799: NHRP: Administrative distance changed to 240`

Examples

The following example shows how to enable all debugging levels for DMVPN tunnel debugging:

```
Router# debug dmvpn all tunnel
```

Related Commands

Command	Description
debug crypto error	Enables error debugging for a crypto area.
debug crypto ipsec	Displays IPsec events.
debug crypto isakmp	Displays messages about IKE events.
debug dmvpn condition	Display conditional debug DMVPN session information.
debug nhrp condition	Enables NHRP conditional debugging.
debug nhrp error	Displays NHRP error-level debugging information.

debug dmvpn condition

To display conditional debug Dynamic Multipoint VPN (DMVPN) session information, use the **debug dmvpn condition** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug dmvpn condition {**unmatched** | **peer** {**nbma** | **tunnel** {*ipv4-address* | *ipv6-address*}} | **vrf** *vrf-name* | **interface tunnel** *tunnel-interface*}

no debug dmvpn condition [**unmatched** | **peer** {**nbma** | **tunnel** {*ipv4-address* | *ipv6-address*}} | **vrf** *vrf-name* | **interface tunnel** *number*]

Syntax Description

unmatched	Specifies debugging when context information is not available.
peer	Specifies information for a specific DMVPN peer.
nbma	Displays DMVPN information based on the peer mapping nonbroadcast access (NBMA) address.
tunnel	Displays DMVPN information based on the peer Virtual Private Network (VPN) address.
ipv4-address	The DMVPN peer IPv4 address.
ipv6-address	The DMVPN peer IPv6 address. **Note** Cisco IOS XE Release 2.5 does not support the *ipv6-address* argument.
vrf	Displays information based on the specified virtual routing and forwarding (VRF) name.
vrf-name	The VRF name.
interface	Displays DMVPN information based on a specific interface.
tunnel	Specifies the tunnel address for a DMVPN peer.
number	The tunnel interface number.

Command Default

DMVPN conditional debugging is disabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(9)T	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.
12.4(20)T	The *ipv6-address* argument was added.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

Conditional debugging is enabled only after the DMVPN debugging type and level have been specified using the **debug dmvpn** command.

Console Output

The following **debug dmvpn** commands do not have any console output on the Cisco 3845 and Cisco 7200 series routers:

- **debug dmvpn condition interface**
- **debug dmvpn condition peer**
- **debug dmvpn condition unmatched**
- **debug dmvpn condition vrf**

Note When the **debug dmvpn condition unmatched** command is enabled on the Cisco 3845 and Cisco 7200 series routers, issuing the **show debugging** command does not produce any console output.

Examples

The following example shows how to enable conditional DMVPN debugging for a specific peer NBMA address:

```
Router# debug dmvpn condition peer nbma 192.0.2.1
```

The following example shows how to enable conditional DMVPN debugging when context is not available to check against debugging conditions:

```
Router# debug dmvpn condition unmatched
```

The following example shows how to disable conditional debugging for a specific tunnel interface:

```
Router# no debug dmvpn condition interface tunnel 1
```

The following example shows how to disable all conditional debugging:

```
Router# no debug dmvpn condition
```

Related Commands

Command	Description
debug crypto error	Enables error debugging for a crypto area.
debug crypto ipsec	Displays IPsec events.
debug crypto isakmp	Displays messages about IKE events.
debug dmvpn	Displays debug DMVPN session information.
debug nhrp condition	Enables NHRP conditional debugging.
debug nhrp error	Displays NHRP error-level debugging information.

debug eigrp fsm

To display debugging information about Enhanced Interior Gateway Routing Protocol (EIGRP) feasible successor metrics (FSMs), use the **debug eigrp fsm** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug eigrp fsm

no debug eigrp fsm

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.4(6)T	Support for IPv6 was added.
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.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

This command helps you observe EIGRP feasible successor activity and to determine whether route updates are being installed and deleted by the routing process.

Examples

The following is sample output from the **debug eigrp fsm** command:

```
Router# debug eigrp fsm

DUAL: dual_rcvupdate(): 172.25.166.0 255.255.255.0 via 0.0.0.0 metric 750080/0
DUAL: Find FS for dest 172.25.166.0 255.255.255.0. FD is 4294967295, RD is 42949
67295 found
DUAL: RT installed 172.25.166.0 255.255.255.0 via 0.0.0.0
DUAL: dual_rcvupdate(): 192.168.4.0 255.255.255.0 via 0.0.0.0 metric 4294967295/
4294967295
DUAL: Find FS for dest 192.168.4.0 255.255.255.0. FD is 2249216, RD is 2249216
DUAL:   0.0.0.0 metric 4294967295/4294967295not found Dmin is 4294967295
DUAL: Dest 192.168.4.0 255.255.255.0 not entering active state.
DUAL: Removing dest 192.168.4.0 255.255.255.0, nexthop 0.0.0.0
DUAL: No routes. Flushing dest 192.168.4.0 255.255.255.0
```

In the first line, DUAL stands for diffusing update algorithm. It is the basic mechanism within EIGRP that makes the routing decisions. The next three fields are the Internet address and mask of the destination network and the address through which the update was received. The metric field shows the metric stored in the routing table and the metric advertised by the neighbor sending the information. If shown, the term “Metric... inaccessible” usually means that the neighbor router no longer has a route to the destination, or the destination is in a hold-down state.

In the following output, EIGRP is attempting to find a feasible successor for the destination. Feasible successors are part of the DUAL loop avoidance methods. The FD field contains more loop avoidance state information. The RD field is the reported distance, which is the metric used in update, query, or reply packets.

The indented line with the "not found" message means a feasible successor (FS) was not found for 192.168.4.0 and EIGRP must start a diffusing computation. This means it begins to actively probe (sends query packets about destination 192.168.4.0) the network looking for alternate paths to 192.164.4.0.

```
DUAL: Find FS for dest 192.168.4.0 255.255.255.0. FD is 2249216, RD is 2249216
DUAL:   0.0.0.0 metric 4294967295/4294967295not found Dmin is 4294967295
```

The following output indicates the route DUAL successfully installed into the routing table:

```
DUAL: RT installed 172.25.166.0 255.255.255.0 via 0.0.0.0
```

The following output shows that no routes to the destination were discovered and that the route information is being removed from the topology table:

```
DUAL: Dest 192.168.4.0 255.255.255.0 not entering active state.
DUAL: Removing dest 192.168.4.0 255.255.255.0, nexthop 0.0.0.0
DUAL: No routes. Flushing dest 192.168.4.0 255.255.255.0
```

debug eigrp neighbor

To display neighbors discovered by the Enhanced Interior Gateway Routing Protocol (EIGRP), use the **debug eigrp neighbor** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug eigrp neighbor [**siatimer**] [**static**]

no debug eigrp neighbor [**siatimer**] [**static**]

Syntax Description

siatimer	(Optional) Stuck-in-active (SIA) timer messages.
static	(Optional) Static routes.

Command Default

Debugging for EIGRP neighbors is not enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.4(6)T	Support for IPv6 was added.
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.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Examples

The following is sample output from the **debug eigrp neighbor** command:

```
Router# debug eigrp neighbor static

EIGRP Static Neighbors debugging is on

Router# configure terminal

Router(config)# router eigrp 100

Router(config-router)# neighbor 10.1.1.1 e3/1

Router(config-router)#
22:40:07:EIGRP:Multicast Hello is disabled on Ethernet3/1!
22:40:07:EIGRP:Add new static nbr 10.1.1.1 to AS 100 Ethernet3/1

Router(config-router)# no neighbor 10.1.1.1 e3/1

Router(config-router)#
22:41:23:EIGRP:Static nbr 10.1.1.1 not in AS 100 Ethernet3/1 dynamic list
22:41:23:EIGRP:Delete static nbr 10.1.1.1 from AS 100 Ethernet3/1
22:41:23:EIGRP:Multicast Hello is enabled on Ethernet3/1!
```

Related Commands

Command	Description
neighbor	Defines a neighboring router with which to exchange routing information.
show ip eigrp neighbors	Displays EIGRP neighbors.
show ipv6 eigrp neighbors	Displays IPv6 EIGRP neighbors.

debug eigrp packet

To display debugging information for Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 packets, use the **debug eigrp packet** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug eigrp packet [**SIAquery** | **SIAreply** | **ack** | **hello** | **ipxsap** | **probe** | **query** | **reply** | **request** | **retry** | **stub** | **terse** | **update** | **verbose**]

no debug eigrp packet

Syntax Description

SIAquery	(Optional) Displays information about Stuck-in-Active (SIA) query messages.
SIAreply	(Optional) Displays information about SIA reply messages.
ack	(Optional) Displays information about EIGRP acknowledgment packets.
hello	(Optional) Displays information about EIGRP hello packets.
ipxsap	(Optional) Displays information about IPX EIGRP SAP packets.
probe	(Optional) Displays information about EIGRP probe packets.
query	(Optional) Displays information about EIGRP query packets.
reply	(Optional) Displays information about EIGRP reply packets.
request	(Optional) Displays information about EIGRP request packets.
retry	(Optional) Displays information about EIGRP retry packets.
stub	(Optional) Displays information about EIGRP stub packets.
terse	(Optional) Displays information about all EIGRP packets except Hello packets.
update	(Optional) Displays information about EIGRP update packets.
verbose	(Optional) Displays information about all EIGRP packets.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.4	The keywords were supported.
12.4(6)T	Support for IPv6 was added.
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.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

If a communication session is closing when it should not be, an end-to-end connection problem can be the cause. The **debug eigrp packet** command is useful for analyzing the messages traveling between the local and remote hosts.

Note Although this command accepts a number of keywords, we don't recommend their use unless directed by TAC.

Examples

The following is sample output from the **debug eigrp packet** command:

```
Router# debug eigrp packet

EIGRP: Sending HELLO on Ethernet0/1
       AS 109, Flags 0x0, Seq 0, Ack 0
EIGRP: Sending HELLO on Ethernet0/1
       AS 109, Flags 0x0, Seq 0, Ack 0
EIGRP: Sending HELLO on Ethernet0/1
       AS 109, Flags 0x0, Seq 0, Ack 0
EIGRP: Received UPDATE on Ethernet0/1 from 192.195.78.24,
       AS 109, Flags 0x1, Seq 1, Ack 0
EIGRP: Sending HELLO/ACK on Ethernet0/1 to 192.195.78.24,
       AS 109, Flags 0x0, Seq 0, Ack 1
EIGRP: Sending HELLO/ACK on Ethernet0/1 to 192.195.78.24,
       AS 109, Flags 0x0, Seq 0, Ack 1
EIGRP: Received UPDATE on Ethernet0/1 from 192.195.78.24,
       AS 109, Flags 0x0, Seq 2, Ack 0
```

The output shows transmission and receipt of EIGRP packets. These packet types may be hello, update, request, query, or reply packets. The sequence and acknowledgment numbers used by the EIGRP reliable transport algorithm are shown in the output. Where applicable, the network-layer address of the neighboring router is also included.

Table 15 describes the significant fields shown in the display.

Table 15 debug eigrp packet Field Descriptions

Field	Description
EIGRP:	EIGRP packet information.
AS n	Autonomous system number.
Flags 0x0	A flag of 1 means the sending router is indicating to the receiving router that this is the first packet it has sent to the receiver. A flag of 2 is a multicast that should be conditionally received by routers that have the conditionally receive (CR) bit set. This bit gets set when the sender of the multicast has previously sent a sequence packet explicitly telling it to set the CR bit.
HELLO	Hello packets are the neighbor discovery packets. They are used to determine whether neighbors are still alive. As long as neighbors receive the hello packets the router is sending, the neighbors validate the router and any routing information sent. If neighbors lose the hello packets, the receiving neighbors invalidate any routing information previously sent. Neighbors also send hello packets.

debug eigrp transmit

To display transmittal messages sent by the Enhanced Interior Gateway Routing Protocol (EIGRP), use the **debug eigrp transmit** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug eigrp transmit [**ack**] [**build**] [**detail**] [**link**] [**packetize**] [**peerdown**] [**sia**] [**startup**] [**strange**]

no debug eigrp transmit [**ack**] [**build**] [**detail**] [**link**] [**packetize**] [**peerdown**] [**sia**] [**startup**] [**strange**]

Syntax Description

ack	(Optional) Information for acknowledgment (ACK) messages sent by the system.
build	(Optional) Build information messages (messages that indicate that a topology table was either successfully built or could not be built).
detail	(Optional) Additional detail for debug output.
link	(Optional) Information regarding topology table linked-list management.
packetize	(Optional) Information regarding topology table linked-list management.
peerdown	(Optional) Information regarding the impact on packet generation when a peer is down.
sia	(Optional) Stuck-in-active (SIA) messages.
startup	(Optional) Information regarding peer startup and initialization packets that have been transmitted.
strange	(Optional) Unusual events relating to packet processing.

Command Default

Debugging for EIGRP transmittal messages is not enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1	This command was introduced.
12.4(6)T	Support for IPv6 was added.
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.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Examples

The following is sample output from the **debug eigrp transmit** command:

```
Router# debug eigrp transmit
```

```
EIGRP Transmission Events debugging is on
    (ACK, PACKETIZE, STARTUP, PEERDOWN, LINK, BUILD, STRANGE, SIA, DETAIL)

Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
Router#(config)# router eigrp 100
Router#(config-router)# network 10.4.9.0 0.0.0.255
Router#(config-router)#
5d22h: DNDB UPDATE 10.0.0.0/8, serno 0 to 1, refcount 0
Router#(config-router)#
```

debug fm ipv6 pbr

To enable IPv6 policy-based routing debugging, use the **debug fm ipv6 pbr** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug fm ipv6 policy [**all** | **events** | **vmrs**]

no debug fm ipv6 policy [**all** | **events** | **vmrs**]

Syntax Description

all	(Optional) Displays all PBR debugging information.
events	(Optional) Displays debugging information about PBR events.
vmrs	(Optional) Displays debugging information about PBR value mask results (VMRs).

Command Default

IPv6 policy-based routing debugging information is not displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(33)SXI4	This command was introduced.

Usage Guidelines

Do not use the **debug fm ipv6 pbr** command unless you suspect a problem with IPv6 policy-based routing.

Examples

The following example enables IPv6 PBR debugging information:

```
Router# debug fm ipv6 pbr
```

debug fm raguard

To display information about router advertisement (RA) guard debugging activity, use the **debug fm raguard** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug fm raguard [**all** | **events** | **error** | **unusual** | **vmr**]

no debug fm raguard

Syntax Description

all	(Optional) All RA guard debugging information is displayed.
events	(Optional) Information about RA guard debugging events is displayed.
error	(Optional) Information about RA guard debugging errors is displayed.
unusual	(Optional) Information about unusual RA guard debugging events is displayed.
vmr	(Optional) Information about debugging value mask results (VMRs) is displayed.

Command Default

RA guard debugging information is not displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(33)SXI4	This command was introduced.
12.2(54)SG	This command was modified. Support for Cisco IOS Release 12.2(54)SG was added.
12.2(50)SY	This command was modified. The **unusual** keyword was added.

Usage Guidelines

Do not use the **debug fm raguard** command unless you suspect a problem with IPv6 RA guard.

Examples

The following example enables you to view IPv6 RA guard debugging activity:

```
Router# debug fm raguard
```

debug ip flow cache

To enable debugging output for NetFlow cache, use the **debug ip flow cache** command in user EXEC or privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ip flow cache

no debug ip flow cache

Syntax Description

This command has no arguments or keywords.

Command Default

Debugging output for NetFlow data export is disabled.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(1)	This command was introduced.
12.3(1)	Debugging output for NetFlow v9 data export was added.
12.3(7)T	Debugging output for NetFlow for IPv6 was added.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)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.

Examples

The following is sample output from the **debug ip flow export** command:

```
Router# debug ip flow cache
IP Flow cache allocation debugging is on

Router# show ipv6 flow

IP packet size distribution (0 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 0 bytes
  0 active, 0 inactive, 0 added
  0 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
SrcAddress                                 InpIf    DstAddress
                OutIf    Prot SrcPrt DstPrt Packets
c7200-vxr-2#
```

```
000037: 01:56:26: IPFLOW: Allocating Sub-Flow cache, without hash flags.
000038: 01:56:26: IPFLOW: Sub-Flow table enabled.
000039: 01:56:26: IPFLOW: Sub-Flow numbers are:
    24 sub-flows per chunk, 0 hashflag len,
    1 chunks allocated, 12 max chunks,
    24 allocated records, 24 free records, 960 bytes allocated
000040: 01:56:26: IPFLOW: Sub-Flow cache removed
```

Related Commands

Command	Description
export destination	Enables the exporting of information from NetFlow aggregation caches.
ip flow-aggregation cache	Enables NetFlow aggregation cache schemes.
ip flow-export	Enables the exporting of information in NetFlow cache entries.
ipv6 flow-aggregation cache	Enables NetFlow aggregation cache schemes for IPv6 configurations.
ipv6 flow export	Enables the exporting of information in NetFlow cache entries for IPv6 NetFlow configurations.
show ip cache flow aggregation	Displays the NetFlow aggregation cache configuration.
show ip flow export	Display the statistics for NetFlow data export.

debug ip flow export

To enable debugging output for NetFlow data export, use the **debug ip flow export** command in user EXEC or privileged EXEC mode. To disable debugging output for NetFlow data export, use the **no** form of this command.

debug ip flow export

no debug ip flow export

Syntax Description

This command has no keywords or arguments.

Command Default

Debugging output for NetFlow data export is disabled.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(1)	This command was introduced.
12.3(1)	Debugging output for NetFlow v9 data export was added.
12.3(7)T	This command was modified so that NetFlow v9 data is collected for both IPv4 and IPv6.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(18)SXF	This command was integrated into Cisco IOS Release 12.2(18)SXF.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following is sample output from the **debug ip flow export** command:

```
Router# debug ip flow export

IP Flow export mechanism debugging is on
*Mar 6 22:56:21.627:IPFLOW:Sending export pak to 2001::FFFE/64 port 9999
*Mar 6 22:56:21.627:IPFLOW:Error sending export packet:Adjacency failure
```

Related Commands

Command	Description
export destination	Enables the exporting of information from NetFlow aggregation caches.
ipv6 flow-aggregation cache	Enables NetFlow aggregation cache schemes for IPv6.
ipv6 flow-export	Enables the exporting of information in NetFlow cache entries.

Command	Description
show ip cache flow aggregation	Displays the NetFlow accounting aggregation cache statistics.
show ip flow export	Displays the statistics for NetFlow data export.
show ipv6 flow export	Displays the statistics for NetFlow data export for IPv6.

debug ipv6 cef drop

To display debug messages for Cisco Express Forwarding for IPv6 (CEFv6) and distributed CEFv6 (dCEFv6) dropped packets, use the **debug ipv6 cef drop** command in privileged EXEC mode. To disable debug messages for CEFv6 and dCEFv6 dropped packets, use the **no** form of this command.

debug ipv6 cef drop [**rpf**]

no debug ipv6 cef drop

Syntax Description

rpf	(Optional) Displays packets dropped by the IPv6 CEF Unicast Reverse-Path Forwarding (Unicast RPF) feature.

Command Default

Debugging for CEFv6 and dCEFv6 dropped packets is not enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(22)S	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(25)S	The **rpf** 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.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **debug ipv6 cef drop** command is similar to the **debug ip cef drops** command, except that it is IPv6-specific.

Note By default, the network server sends the output from **debug** commands and system error messages to the console. To redirect debug output, use the **logging** command options in global configuration mode. Destinations include the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server. For complete information on **debug** commands and redirecting debug output, refer to the Release 12.3 *Cisco IOS Debug Command Reference*.

Examples

The following is sample output from the **debug ipv6 cef drop** command:

```
Router# debug ipv6 cef drop

*Aug 30 08:20:51.169: IPv6-CEF: received packet on Serial6/0/2
*Aug 30 08:20:51.169: IPv6-CEF: found no adjacency for 2001:0DB8::1 reason 2
*Aug 30 08:20:51.169: IPv6-CEF: packet not switched: code 0x1
```

Table 16 describes the significant fields shown in the display.

Table 16 debug ipv6 cef drop Field Descriptions

Field	Description
IPv6-CEF: received packet on Serial6/0/2	Cisco Express Forwarding has received a packet addressed to the router via serial interface 6/0/2.
IPv6-CEF: found no adjacency for 2001:0DB8::1	Cisco Express Forwarding has found no adjacency for the IPv6 address prefix of 2001:0DB8::1.
IPv6-CEF: packet not switched	Cisco Express Forwarding has dropped the packet.

Related Commands

Command	Description
debug ipv6 cef events	Displays debug messages for CEFv6 and dCEFv6 general events.
debug ipv6 cef table	Displays debug messages for CEFv6 and dCEFv6 table modification events.

debug ipv6 cef events

To display debug messages for Cisco Express Forwarding for IPv6 (CEFv6) and distributed CEFv6 (dCEFv6) general events, use the **debug ipv6 cef events** command in privileged EXEC mode. To disable debug messages for CEFv6 and dCEFv6 general events, use the **no** form of this command.

debug ipv6 cef events

no debug ipv6 cef events

Syntax Description

This command has no arguments or keywords.

Command Default

Debugging for CEFv6 and dCEFv6 general events is not enabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(22)S	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(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.

Usage Guidelines

The **debug ipv6 cef events** command is similar to the **debug ip cef events** command, except that it is IPv6-specific.

Note By default, the network server sends the output from debug commands and system error messages to the console. To redirect debug output, use the logging command options in global configuration mode. Destinations include the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server. For complete information on **debug** commands and redirecting debug output, refer to the Release 12 *Cisco IOS Debug Command Reference*.

Examples

The following is sample output from the **debug ipv6 cef events** command:

```
Router# debug ipv6 cef events

IPv6 CEF packet events debugging is on
Router#
*Aug 30 08:22:57.809: %LINK-3-UPDOWN: Interface Serial6/0/2, changed state to up
*Aug 30 08:22:58.809: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial6/0/2, changed
state to up
*Aug 30 08:23:00.821: CEFv6-IDB: Serial6/0/2 address 2001:0DB8::248 add download succeeded
```

Table 17 describes the significant fields shown in the display.

Table 17 debug ipv6 cef events Field Descriptions

Field	Description
Interface Serial6/0/2, changed state to up	Indicates that the interface hardware on serial interface 6/0/2 is currently active.
Line protocol on Interface Serial6/0/2, changed state to up	Indicates that the software processes that handle the line protocol consider the line usable for serial interface 6/0/2.
Serial6/0/2 address 2001:0DB8::248 add download succeeded	The IPv6 address 2001:0DB8::248 was downloaded successfully.

Related Commands

Command	Description
debug ipv6 cef table	Displays debug messages for CEFv6 and dCEFv6 table modification events.

debug ipv6 cef hash

To display debug messages for Cisco Express Forwarding for IPv6 (CEFv6) and distributed CEFv6 (dCEFv6) load-sharing hash algorithm events, use the **debug ipv6 cef hash** command in privileged EXEC mode. To disable debug messages for CEFv6 and dCEFv6 load-sharing hash algorithm events, use the **no** form of this command.

debug ipv6 cef hash

no debug ipv6 cef hash

Syntax Description

This command has no arguments or keywords.

Command Default

Debugging for CEFv6 and dCEFv6 load-sharing hash algorithm events is not enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(22)S	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(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.

Usage Guidelines

The **debug ipv6 cef hash** command is similar to the **debug ip cef hash** command, except that it is IPv6-specific.

Use this command when changing the load-sharing algorithm to display IPv6 hash table details.

Note By default, the network server sends the output from debug commands and system error messages to the console. To redirect debug output, use the logging command options in global configuration mode. Destinations include the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server.

Related Commands

Command	Description
debug ipv6 cef events	Displays debug messages for CEFv6 and dCEFv6 general events.
debug ipv6 cef table	Displays debug messages for CEFv6 and dCEFv6 table modification events.

debug ipv6 cef receive

To display debug messages for Cisco Express Forwarding for IPv6 (CEFv6) and distributed CEFv6 (dCEFv6) packets that are process-switched on the router, use the **debug ipv6 cef receive** command in privileged EXEC mode. To disable debug messages for CEFv6 and dCEFv6 packets that are process-switched on the router, use the **no** form of this command.

debug ipv6 cef receive

no debug ipv6 cef receive

Syntax Description

This command has no arguments or keywords.

Command Default

Debugging for CEFv6 and dCEFv6 packets that are process-switched on the router is not enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(22)S	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(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.

Usage Guidelines

The **debug ipv6 cef receive** command is similar to the **debug ip cef receive** command, except that it is IPv6-specific.

Note By default, the network server sends the output from debug commands and system error messages to the console. To redirect debug output, use the logging command options in global configuration mode. Destinations include the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server. For complete information on debug commands and redirecting debug output, refer to the Release 12 *Cisco IOS Debug Command Reference*.

Examples

The following is sample output from the **debug ipv6 cef receive** command when another router in the network pings 2001:0DB8::2 which is a local address on this box:

```
Router# debug ipv6 cef receive

IPv6 CEF packet receives debugging is on
router#
*Aug 30 08:25:14.869: IPv6CEF-receive: Receive packet for 2001:0DB8::2
```

```
*Aug 30 08:25:14.897: IPv6CEF-receive: Receive packet for 2001:0DB8::2
*Aug 30 08:25:14.925: IPv6CEF-receive: Receive packet for 2001:0DB8::2
*Aug 30 08:25:14.953: IPv6CEF-receive: Receive packet for 2001:0DB8::2
*Aug 30 08:25:14.981: IPv6CEF-receive: Receive packet for 2001:0DB8::2
```

Table 18 describes the significant fields shown in the display.

Table 18 debug ipv6 cef receive Field Descriptions

Field	Description
IPv6CEF-receive: Receive packet for 2001:0DB8::2	Cisco Express Forwarding has received a packet addressed to the router.

Related Commands

Command	Description
debug ipv6 cef events	Displays debug messages for CEFv6 and dCEFv6 general events.
debug ipv6 cef table	Displays debug messages for CEFv6 and dCEFv6 table modification events.

debug ipv6 cef table

To display debug messages for Cisco Express Forwarding for IPv6 (CEFv6) and distributed CEFv6 (dCEFv6) table modification events, use the **debug ipv6 cef table** command in privileged EXEC mode. To disable debug messages for CEFv6 and dCEFv6 table modification events, use the **no** form of this command.

debug ipv6 cef table [**background**]

no debug ipv6 cef table [**background**]

Syntax Description

background	(Optional) Sets CEFv6 and dCEFv6 table background updates.

Command Default

Debugging for CEFv6 and dCEFv6 table modification events is not enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(22)S	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(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.

Usage Guidelines

The **debug ipv6 cef table** command is similar to the **debug ip cef table** command, except that it is IPv6-specific.

This command is used to record CEFv6 and dCEFv6 table events related to the Forwarding Information Base (FIB) tables. Types of events include the following:

- Routing updates that populate the FIB tables
- Flushing of the FIB tables
- Adding or removing of entries to the FIB tables
- Table reloading process

Note By default, the network server sends the output from debug commands and system error messages to the console. To redirect debug output, use the logging command options in global configuration mode. Destinations include the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server. For complete information on debug commands and redirecting debug output, refer to the *Cisco IOS Debug Command Reference*.

Examples

The following is sample output from the **debug ipv6 cef table** command when a static route is added:

```
Router# debug ipv6 cef table

IPv6 CEF table debugging is on

router(config)# ipv6 route 5555::/64 serial 2/0 3000::2
router(config)#
*Feb 24 08:46:09.187: IPv6CEF-Table: Event add, 5555::/64
*Feb 24 08:46:09.187: IPv6 CEF table: Created path_list 01184570
*Feb 24 08:46:09.187: IPv6 CEF table: Adding path 01181A80 to path_list 01184570 old path
count=0
*Feb 24 08:46:09.187: IPv6 CEF table: No matching list for path list 01184570
*Feb 24 08:46:09.187: IPv6 CEF table: Adding fib entry 0117EE80 to path_list 01184570 old
refcount=0
*Feb 24 08:46:09.187: IPv6 CEF table: Added path_list 01184570 to hash 50
*Feb 24 08:46:09.187: IPv6 CEF: Linking path 01181A80 to adjacency 01138E28
*Feb 24 08:46:09.187: IPv6 CEF table: Created 0 loadinfos for path_list 01184570
*Feb 24 08:46:09.187: IPv6CEF-Table: Validated 5555::/64
```

The following is sample output when the static route is removed:

```
router(config)# no ipv6 route 5555::/64 serial 2/0 3000::2
router(config)#
*Feb 24 08:46:43.871: IPv6CEF-Table: Event delete, 5555::/64
*Feb 24 08:46:43.871: IPv6CEF-Table: Invalidated 5555::/64
*Feb 24 08:46:43.871: IPv6CEF-Table: Deleted 5555::/64
*Feb 24 08:46:43.871: IPv6 CEF table: Removing fib entry 0117EE80 from path_list 01184570
old refcount=1
*Feb 24 08:46:43.871: IPv6 CEF table: Removed path_list 01184570 from hash 50
*Feb 24 08:46:43.871: IPv6 CEF table: Freeing path_list 01184570 refcount=0
*Feb 24 08:46:43.871: IPv6 CEF table: Freeing all 1 paths in path_list 01184570
*Feb 24 08:46:43.871: IPv6 CEF: deleting path 01181A80
```

Related Commands

Command	Description
debug ipv6 cef events	Displays debug messages for CEFv6 and dCEFv6 general events.

debug fm raguard

To enable debugging for IPv6 router advertisement (RA) guard, use the **debug fm raguard** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug fm raguard [**all** | **error** | **events** | **vmr**]

no debug fm raguard

Syntax Description

all	(Optional) Displays all RA guard information.
error	(Optional) Displays information about RA guard errors.
events	(Optional) Displays information about RA guard events.
vmr	(Optional) Displays information about variable-rate multimode (VMR) generation in RA guard.

Command Default

Debugging for the DHCP for IPv6 is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

The **debug fm raguard** command is used to show debug information related to the RA guard.

Examples

The following example enables debugging for RA guard for IPv6:

```
Router# debug fm raguard
```

debug ipv6 dhcp database

To enable debugging for the Dynamic Host Configuration Protocol (DHCP) for IPv6 binding database agent, use the **debug ipv6 dhcp database** command in privileged EXEC mode. To disable the display of debug messages for the DHCP for IPv6 binding database agent, use the **no** form of this command.

debug ipv6 dhcp database

no debug ipv6 dhcp database

Syntax Description

This command has no keywords or arguments.

Command Default

Debugging for the DHCP for IPv6 binding database agent is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

The **debug ipv6 dhcp database** command enables debugging for DHCP for IPv6 database processing.

Examples

The following example enables debugging for the DHCP for IPv6 binding database agent:

```
Router# debug ipv6 dhcp database
```

Related Commands

Command	Description
debug ipv6 dhcp	Enables debugging for DHCP for IPv6.

debug ipv6 dhcp relay

To enable DHCP for IPv6 relay agent debugging, use the **debug ipv6 dhcp relay** command in user EXEC or privileged EXEC mode. To disable DHCP for IPv6 relay agent debugging, use the **no** form of this command.

debug ipv6 dhcp relay [**bulk-lease**]

no debug ipv6 dhcp relay [**bulk-lease**]

Syntax Description

bulk-lease	(Optional) Enables bulk lease query debugging flows.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.3(11)T	This command was introduced.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.1(1)S	This command was modified. The **bulk-lease** keyword was added.

Usage Guidelines

The DHCP functions for IPv6 client, server, and relay agent are mutually exclusive on an interface. When one of these functions is enabled and a user tries to configure a different function on the same interface, one of the following messages is displayed: Interface is in DHCP client mode, Interface is in DHCP server mode, or Interface is in DHCP relay mode.

Examples

The following example enables DHCP for IPv6 relay agent debugging:

```
Router# debug ipv6 dhcp relay
```

Related Commands

Command	Description
debug ipv6 dhcp	Enables DHCP debugging for IPv6.

debug ipv6 eigrp

To display information about the Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 protocol, use the **debug ipv6 eigrp** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ipv6 eigrp [*as-number*] [**neighbor** *ipv6-address* | **notification** | **summary**]

no debug ipv6 eigrp

Syntax Description

as-number	(Optional) Autonomous system number.
neighbor *ipv6-address*	(Optional) IPv6 address of the neighboring router.
notification	(Optional) Displays EIGRP for IPv6 events and notifications in the console of the router.
summary	(Optional) Displays a summary of EIGRP for IPv6 routing information.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(6)T	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.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

Because the **debug ipv6 eigrp** command generates a substantial amount of output, use it only when traffic on the network is light.

Examples

The following example enables debugging output:

```
Router# debug ipv6 eigrp
```

debug ipv6 icmp

To display debugging messages for IPv6 Internet Control Message Protocol (ICMP) transactions (excluding IPv6 ICMP neighbor discovery transactions), use the **debug ipv6 icmp** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ipv6 icmp

no debug ipv6 icmp

Syntax Description

This command has no arguments or keywords.

Command Default

Debugging for IPv6 ICMP is not enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)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 Release 12.2(14)S.
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.
12.2(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.
12.2(33)SB	This command's output was modified on the Cisco 10000 series router for the PRE3 and PRE4.

Usage Guidelines

The **debug ipv6 icmp** command is similar to the **debug ip icmp** command, except that it is IPv6-specific.

Note By default, the network server sends the output from **debug** commands and system error messages to the console. To redirect debugging output, use the logging command options in global configuration mode. Destinations include the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server.

This command helps you determine whether the router is sending or receiving IPv6 ICMP messages. Use it, for example, when you are troubleshooting an end-to-end connection problem.

Note For more information about the fields in **debug ipv6 icmp** output, refer to RFC 2463, *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6).*

Cisco 10000 Series Router Usage Guidelines

In Cisco IOS Release 12.2(33)SB, output from the **debug ipv6 icmp** command displays information similar to the following:

```
ICMPv6: Received echo reply from 2010:1:1:1:1:1:1:2
```

In Cisco IOS Release 12.2(31)SB, the **debug ipv6 icmp** command output displays information similar to the following:

```
ICMPv6: Received ICMPv6 packet from 2010:1:1:1:1:1:1:2, type 129
```

Examples

The following is sample output from the **debug ipv6 icmp** command:

```
Router# debug ipv6 icmp

13:28:40:ICMPv6:Received ICMPv6 packet from 2000:0:0:3::2, type 136
13:28:45:ICMPv6:Received ICMPv6 packet from FE80::203:A0FF:FED6:1400, type 135
13:28:50:ICMPv6:Received ICMPv6 packet from FE80::203:A0FF:FED6:1400, type 136
13:28:55:ICMPv6:Received ICMPv6 packet from FE80::203:A0FF:FED6:1400, type 135
```

Table 19 describes significant fields shown in the first line of the display.

Table 19 debug ipv6 icmp Field Descriptions

Field	Description
13:28:40:	Indicates the time (hours:minutes:seconds) at which the ICMP neighbor discovery event occurred.
*n*w*n*d: (not shown in sample output)	Indicates time (weeks, days) since last reboot of the event occurring. For example, 1w4d: indicates the time (since the last reboot) of the event occurring was 1 week and 4 days ago.
ICMPv6:	Indication that this message describes an ICMP version 6 packet.
Received ICMPv6 packet from 2000:0:0:3::2	IPv6 address from which the ICMP version 6 packet is received.
type 136	The number variable indicates one of the following IPv6 ICMP message types: • 1—Destination unreachable. The router cannot forward a packet that was sent or received. • 2—Packet too big. The router attempts to send a packet that exceeds the maximum transmission unit (MTU) of a link between itself and the packet destination. • 3—Time exceeded. Either the hop limit in transit or the fragment reassembly time is exceeded. • 4—Parameter problem. The router attempts to send an IPv6 packet that contains invalid parameters. An example is a packet containing a next header type unsupported by the router that is forwarding the packet. • 128—Echo request. The router received an echo reply. • 129—Echo reply. The router sent an echo reply. • 133—Router solicitation messages. Hosts send these messages to prompt routers on the local link to send router advertisement messages. • 134—Router advertisement messages. Routers periodically send these messages to advertise their link-layer addresses, prefixes for the link, and other link-specific information. These messages are also sent in response to router solicitation messages. • 135—Neighbor solicitation messages. Nodes send these messages to request the link-layer address of a station on the same link. • 136—Neighbor advertisement messages. Nodes send these messages, containing their link-local addresses, in response to neighbor solicitation messages. • 137—Redirect messages. Routers send these messages to hosts when a host attempts to use a less-than-optimal first hop address when forwarding packets. These messages contain a better first hop address that should be used instead.

Following are examples of the IPv6 ICMP messages types that can be displayed by the **debug ipv6 icmp** command:

- ICMP echo request and ICMP echo reply messages. In the following example, an ICMP echo request is sent to address 2052::50 and an ICMP echo reply is received from address 2052::50.

```
1w4d:ICMPv6:Sending echo request to 2052::50
1w4d:ICMPv6:Received echo reply from 2052::50
```

- ICMP packet too big messages. In the following example, a router tried to forward a packet to destination address 2052::50 via the next hop address 2052::52. The size of the packet was greater than 1280 bytes, which is the MTU of destination address 2052::50. As a result, the router receives an ICMP packet too big message from the next hop address 2052::52.

```
1w4d:Received ICMP too big from 2052::52 about 2052::50, MTU=1300
```

- ICMP parameter problem messages. In the following example, an ICMP parameter problem message is received from address 2052::52.

```
1w4d:Received ICMP parameter problem from 2052::52
```

- ICMP time exceeded messages. In the following example, an ICMP time exceeded message is received from address 2052::52.

```
1w4d:Received ICMP time exceeded from 2052::52
```

- ICMP unreachable messages. In the following example, an ICMP unreachable message with code 1 is received from address 2052::52. Additionally, an ICMP unreachable message with code 1 is sent to address 2060::20 about address 2062::20.

```
1w4d:Received ICMP unreachable code 1 from 2052::52
1w4d:Sending ICMP unreachable code 1 to 2060::20 about 2062::20
```

Table 20 lists the codes for ICMP unreachable messages.

Table 20 ICMP Unreachable Messages—Code Descriptions

Code	Description
0	The router has no route to the packet destination.
1	Although the router has a route to the packet destination, communication is administratively prohibited.
3	The address is unreachable.
4	The port is unreachable.

Related Commands

Command	Description
debug ipv6 nd	Displays debugging messages for IPv6 ICMP neighbor discovery transactions.

debug ipv6 inspect

To display messages about Cisco IOS firewall events, use the **debug ipv6 inspect** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ipv6 inspect {**function-trace** | **object-creation** | **object-deletion** | **events** | **timers** | **protocol** | **detailed**}

no debug ipv6 inspect detailed

Syntax Description

function-trace	Displays messages about software functions called by the Cisco IOS firewall.
object-creation	Displays messages about software objects being created by the Cisco IOS firewall. Object creation corresponds to the beginning of Cisco IOS firewall-inspected sessions.
object-deletion	Displays messages about software objects being deleted by the Cisco IOS firewall. Object deletion corresponds to the closing of Cisco IOS firewall-inspected sessions.
events	Displays messages about Cisco IOS firewall software events, including information about Cisco IOS firewall packet processing.
timers	Displays messages about Cisco IOS firewall timer events such as when a Cisco IOS firewall idle timeout is reached.
protocol	Displays messages about Cisco IOS firewall-inspected protocol events, including details about the protocol's packets.
detailed	Use this form of the command in conjunction with other Cisco IOS firewall debugging commands. This causes detailed information to be displayed for all the other enabled Cisco IOS firewall debugging.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced
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 Release 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.

Examples

The following example enables the display of messages about Cisco IOS firewall events:

```
debug ipv6 inspect
```

Related Commands

Command	Description
ipv6 inspect audit-trail	Turns on CBAC audit trail messages, which are displayed on the console after each Cisco IOS firewall session closes.
ipv6 inspect name	Defines a set of ipv6 inspection rules.
show ipv6 inspect	Displays CBAC configuration and session information.

debug ipv6 mfib

To enable debugging output on the IPv6 Multicast Forwarding Information Base (MFIB), use the **debug ipv6 mfib** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ipv6 mfib [**vrf** *vrf-name*] [*group-name* | *group-address*] [**adjacency** | **db** | **fs** | **init** | **interface** | **mrib** [**detail**] | **nat** | **pak** | **platform** | **ppr** | **ps** | **signal** | **table**]

no debug ipv6 mfib

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
group-name | *group-address*	(Optional) IPv6 address, name, or interface of the multicast group as defined in the Domain Name System (DNS) hosts table.
adjacency	(Optional) Enables debugging output for adjacency management activity.
db	(Optional) Enables debugging output for route database management activity.
fs	(Optional) Enables debugging output for fast switching activity.
init	(Optional) Enables debugging output for initialization or deinitialization activity.
interface	(Optional) Enables debugging output for IPv6 MFIB interfaces.
mrib	(Optional) Enables debugging output for communication with the MRIB.
detail	(Optional) Enables detailed debugging output regarding the MRIB.
nat	(Optional) Enables debugging output for Network Address Translation (NAT) events associated with all tables.
pak	(Optional) Enables debugging output for packet forwarding activity.
platform	(Optional) Enables debugging output related to the hardware platform use of application program interfaces (APIs).
ppr	(Optional) Enables debugging output for packet preservation events.
ps	(Optional) Enables debugging output for process-level-only packet forwarding activity.
signal	(Optional) Enables debugging output for activity regarding MFIB data-driven signaling to routing protocols.
table	(Optional) Enables debugging output for IPv6 MFIB table activity.

Command Modes

Privileged EXEC

Syntax Description

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)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 introduced on Cisco ASR 1000 series routers.
12.2(33)SRE	The **detail** keyword was added.
15.1(1)T	The **detail** keyword was added.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

If no keywords are used, all IPbv6 MFIB activity debugging output is displayed.

Examples

The following example enables debugging output for adjacency management activity on the IPv6 MFIB:

```
Router# debug ipv6 mfib adjacency
```

debug ipv6 mld

To enable debugging on Multicast Listener Discovery (MLD) protocol activity, use the **debug ipv6 mld** command in privileged EXEC mode. To restore the default value, use the **no** form of this command.

debug ipv6 mld [*group-name* | *group-address* | *interface-type*]

no debug ipv6 mld [*group-name* | *group-address* | *interface-type*]

Cisco IOS Release 12.0(26)S

debug ipv6 mld [**group** *group-name* | *group-address* | **interface** *interface-type*]

no debug ipv6 mld [**group** *group-name* | *group-address* | **interface** *interface-type*]

Syntax Description

group-name | *group-address* or **group** *group-name* | *group-address*	(Optional) IPv6 address or name of the multicast group.
interface-type or **interface** *interface-type*	(Optional) Interface type. For more information, use the question mark (**?**) online help function.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
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.
12.2(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 introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

This command helps discover whether the MLD protocol activities are working correctly. In general, if MLD is not working, the router process never discovers that there is a host on the network that is configured to receive multicast packets.

The messages displayed by the **debug ipv6 mld** command show query and report activity received from other routers and hosts. Use this command in conjunction with **debug ipv6 pim** to display additional multicast activity, to learn more information about the multicast routing process, or to learn why packets are forwarded out of particular interfaces.

Examples

The following example enables debugging on MLD protocol activity:

```
Router# debug ipv6 mld
```

Related Commands

Command	Description
debug ipv6 pim	Enables debugging on PIM protocol activity.

debug ipv6 mld explicit

To display information related to the explicit tracking of hosts, use the **debug ipv6 mld explicit** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug ipv6 mld explicit [*group-name* | *group-address*]

no debug ipv6 mld explicit [*group-name* | *group-address*]

Syntax Description

group-name | *group-address*	(Optional) IPv6 address or name of the multicast group.

Command Default

Debugging for the explicit tracking of hosts is not enabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
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.
12.2(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 introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

When the optional *group-name* or *group-address* argument is not used, all debugging information is displayed.

Examples

The following example shows how to enable information to be displayed about the explicit tracking of hosts. The command output is self-explanatory:

```
Router# debug ipv6 mld explicit

00:00:56:MLD:ET host FE80::A8BB:CCFF:FE00:800 report for FF05::6 (0 srcs) on Ethernet1/0
00:00:56:MLD:ET host FE80::A8BB:CCFF:FE00:800 switch to exclude for FF05::6 on Ethernet1/0
00:00:56:MLD:ET MRIB modify for (*,FF05::6) on Ethernet1/0 new 100, mdf 100
```

debug ipv6 mld ssm-map

To display debug messages for Source Specific Multicast (SSM) mapping related to Multicast Listener Discovery (MLD), use the **debug ipv6 mld ssm-map** command in privileged EXEC mode. To disable debug messages for SSM mapping, use the **no** form of this command.

debug ipv6 mld ssm-map [*source-address*]

no debug ipv6 mld ssm-map [*source-address*]

Syntax Description

source-address	(Optional) Source address associated with an MLD membership for a group identified by the access list.

Command Modes

Privileged EXEC

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

Consult Cisco technical support before using this command.

Examples

The following example allows debugging information for SSM mapping to be displayed:

```
Router# debug ipv6 mld ssm-map
```

Related Commands

Command	Description
ipv6 mld ssm-map enable	Enables the SSM mapping feature for groups in the configured SSM range
ipv6 mld ssm-map query dns	Enables DNS-based SSM mapping.
ipv6 mld ssm-map static	Configures static SSM mappings.
show ipv6 mld ssm-map	Displays SSM mapping information.

debug ipv6 mobile

To enable the display of debugging information for Mobile IPv6, use the **debug ipv6 mobile** command in privileged EXEC mode.

debug ipv6 mobile {**binding-cache** | **forwarding** | **home-agent** | **registration**}

Syntax Description

binding-cache	Events associated with the binding cache.
forwarding	Events associated with forwarding (tunneling) packets for which the router is acting as home agent.
home-agent	Events associated with the home agent, Dynamic Home Address Agent Discovery (DHAAD), Mobile prefix discovery (MPD), and generic home agent (HA) debugging and binding acknowledgments.
registration	Events associated with binding updates that are registrations.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

The **debug ipv6 mobile** command enables the display of selected debugging information. You may use multiple command lines to enable concurrent debugging of multiple classes of information.

Examples

In the following example, debugging information is displayed for binding updates processing:

```
Router# debug ipv6 mobile registration
```

Related Commands

Command	Description
binding	Configures binding options for the Mobile IPv6 home agent feature in home-agent configuration mode.
ipv6 mobile home-agent (global configuration)	Enters home agent configuration mode.
ipv6 mobile home-agent (interface configuration)	Initializes and start the IPv6 Mobile home agent on a specific interface.
ipv6 mobile home-agent preference	Configures the home agent preference value on the interface.

debug ipv6 mobile networks

To display debugging messages for IPv6 mobile networks, use the **debug ipv6 mobile networks** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ipv6 mobile networks

no debug ipv6 mobile networks

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

The **debug ipv6 mobile networks** command enables the display of selected debugging information.

Examples

The following example shows how to enable the display of debugging messages for IPv6 mobile networks:

```
Router# debug ipv6 mobile networks
```

Related Commands

Command	Description
ipv6 mobile router	Enables IPv6 NEMO functionality on a router and places the router in IPv6 mobile router configuration mode.

debug ipv6 mobile router

To display debugging messages for the IPv6 mobile router, use the **debug ipv6 mobile router** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ipv6 mobile router [**detail**]

no debug ipv6 mobile router

Syntax Description

detail	(Optional) Displays detailed mobile router debug messages.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

The IPv6 mobile router operations can be debugged. The following conditions trigger debugging messages:

- Agent discovery
- Registration
- Mobile router state change
- Routes and tunnels created or deleted
- Roaming information

Debugging messages are prefixed with “MobRtr,” and detail messages are prefixed with “MobRtrX.”

Examples

The following example shows how to enable the display of debugging messages for the IPv6 mobile router:

```
Router# debug ipv6 mobile router
```

Related Commands

Command	Description
ipv6 mobile router	Enables IPv6 NEMO functionality on a router and places the router in IPv6 mobile router configuration mode.

debug ipv6 mrib client

To enable debugging on Multicast Routing Information Base (MRIB) client management activity, use the **debug ipv6 mrib client** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ipv6 mrib [**vrf** *vrf-name*] **client**

no debug ipv6 mrib client

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
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.
12.2(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 introduced on Cisco ASR 1000 Series Routers.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

The **debug ipv6 mrib client** command is used to display the activity in the MRIB associated with clients such as Protocol Independent Multicast (PIM) and Multicast Listener Discovery (MLD). If you are having difficulty with your client connections, use this command to display new clients being added and deleted.

The **debug ipv6 mrib client** command also displays information on when a new client is added to or deleted from the MRIB, when a client connection is established or torn down, when a client binds to a particular MRIB table, and when a client is informed that there are updates to be read.

Examples

The following example enables debugging on MRIB client management activity:

```
Router# debug ipv6 mrib client
```

Related Commands

Command	Description
debug ipv6 mrib route	Displays MRIB routing entry-related activity.

debug ipv6 mrib io

To enable debugging on Multicast Routing Information Base (MRIB) I/O events, use the **debug ipv6 mrib io** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ipv6 mrib [**vrf** *vrf-name*] **io**

no debug ipv6 mrib io

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
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.
12.2(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 introduced on Cisco ASR 1000 Series Routers.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

Use the **debug ipv6 mrib io** command to display information on when clients open and close MRIB I/O connections, when MRIB entry and interface updates are received and processed from clients, and when MRIB entry and interface updates are sent to clients.

Examples

The following example enables debugging on MRIB I/O events:

```
Router# debug ipv6 mrib io
```

debug ipv6 mrib proxy

To enable debugging on multicast routing information base (MRIB) proxy activity between the route processor and line cards on distributed router platforms, use the **debug ipv6 mrib proxy** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ipv6 mrib proxy

no debug ipv6 mrib proxy

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

Use the **debug ipv6 mrib proxy** command to display information on connections that are being opened and closed and on MRIB transaction messages that are being passed between the route processor and line cards.

Examples

The following example enables debugging on MRIB proxy events:

```
Router# debug ipv6 mrib proxy
```

debug ipv6 mrib route

To display information about Multicast Routing Information Base (MRIB) routing entry-related activity, use the **debug ipv6 mrib route** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ipv6 mrib [**vrf** *vrf-name*] **route** [*group-name* | *group-address*]

no debug ipv6 mrib route

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
group-name | *group-address*	(Optional) IPv6 address or name of the multicast group.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
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.
12.2(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 introduced on Cisco ASR 1000 Series Routers.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

This command displays update information related to the route database made by MRIB clients, which is then redistributed to the clients.

Use this command to monitor MRIB route activity when discontinuity is found between the MRIB and the client database or between the individual client databases.

Examples

The following example enables the display of information about MRIB routing entry-related activity:

```
Router# debug ipv6 mrib route
```

Related Commands

Command	Description
show ipv6 mrib client	Displays information about the MRIB client management activity.

debug ipv6 mrib table

To enable debugging on Multicast Routing Information Base (MRIB) table management activity, use the **debug ipv6 mrib table** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ipv6 mrib [**vrf** *vrf-name*] **table**

no debug ipv6 mrib table

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
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.
12.2(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 introduced on Cisco ASR 1000 Series Routers.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

Use the **debug ipv6 mrib table** command to display information on new MRIB tables being added and deleted.

Examples

The following example enables debugging on MRIB table management activity:

```
Router# debug ipv6 mrib table
```

debug ipv6 nat

To display debug messages for Network Address Translation—Protocol Translation (NAT-PT) translation events, use the **debug ipv6 nat** command in privileged EXEC mode. To disable debug messages for NAT-PT translation events, use the **no** form of this command.

debug ipv6 nat [**detailed** | **port**]

no debug ipv6 nat [**detailed** | **port**]

Syntax Description

detailed	(Optional) Displays detailed information about NAT-PT translation events.
port	(Optional) Displays port allocation events.

Command Default

Debugging for NAT-PT translation events is not enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.3(2)T	The **port** keyword was added to support Port Address Translation (PAT), or overload, multiplexing multiple IPv6 addresses to a single IPv4 address or to an IPv4 address pool.

Usage Guidelines

The **debug ipv6 nat** command can be used to troubleshoot NAT-PT translation issues. If no keywords are specified, debugging messages for all NAT-PT protocol translation events are displayed.

Note By default, the network server sends the output from **debug** commands and system error messages to the console. To redirect debugging output, use the logging command options within global configuration mode. Destinations are the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server.

Caution Because the **debug ipv6 nat** command generates a substantial amount of output, use it only when traffic on the IPv6 network is low, so other activity on the system is not adversely affected.

Examples

The following example shows output for the **debug ipv6 nat** command:

```
Router# debug ipv6 nat

00:06:06: IPv6 NAT: icmp src (3002::8) -> (192.168.124.8), dst (2001::2) ->
(192.168.123.2)
00:06:06: IPv6 NAT: icmp src (192.168.123.2) -> (2001::2), dst (192.168.124.8) ->
(3002::8)
00:06:06: IPv6 NAT: icmp src (3002::8) -> (192.168.124.8), dst (2001::2) ->
(192.168.123.2)
00:06:06: IPv6 NAT: icmp src (192.168.123.2) -> (2001::2), dst (192.168.124.8) ->
(3002::8)
00:06:06: IPv6 NAT: tcp src (3002::8) -> (192.168.124.8), dst (2001::2) -> (192.168.123.2)
00:06:06: IPv6 NAT: tcp src (192.168.123.2) -> (2001::2), dst (192.168.124.8) -> (3002::8)
00:06:06: IPv6 NAT: tcp src (3002::8) -> (192.168.124.8), dst (2001::2) -> (192.168.123.2)
00:06:06: IPv6 NAT: tcp src (3002::8) -> (192.168.124.8), dst (2001::2) -> (192.168.123.2)
00:06:06: IPv6 NAT: tcp src (3002::8) -> (192.168.124.8), dst (2001::2) -> (192.168.123.2)
00:06:06: IPv6 NAT: tcp src (192.168.123.2) -> (2001::2), dst (192.168.124.8) -> (3002::8)
```

Table 21 describes the significant fields shown in the display.

Table 21 debug ipv6 nat Field Descriptions

Field	Description
IPv6 NAT:	Indicates that this is a NAT-PT packet.
icmp	Protocol of the packet being translated.
src (3000::8) -> (192.168.124.8)	The source IPv6 address and the NAT-PT mapped IPv4 address. **Note** If mapping IPv4 hosts to IPv6 hosts the first address would be an IPv4 address, and the second address an IPv6 address.
dst (2001::2) -> (192.168.123.2)	The destination IPv6 address and the NAT-PT mapped IPv4 address. **Note** If mapping IPv4 hosts to IPv6 hosts the first address would be an IPv4 address, and the second address an IPv6 address.

The following example shows output for the **debug ipv6 nat** command with the **detailed** keyword:

```
Router# debug ipv6 nat detailed

00:14:12: IPv6 NAT: address allocated 192.168.124.8
00:14:16: IPv6 NAT: deleted a NAT entry after timeout
```

debug ipv6 nd

To display debug messages for IPv6 Internet Control Message Protocol (ICMP) neighbor discovery transactions, use the **debug ipv6 nd** command in privileged EXEC mode. To disable debug messages for IPv6 ICMP neighbor discovery transactions, use the **no** form of this command.

debug ipv6 nd

no debug ipv6 nd

Syntax Description

This command has no arguments or keywords.

Command Default

Debugging for IPv6 ICMP neighbor discovery is not enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(4)T	The DAD: <*nnnn*::*nn*:> is unique, DAD: duplicate link-local <*nnnn*::*nn*:> on <*interface type*>, interface stalled, and Received NA for <*nnnn*::*nn*:> on <*interface type*> from <*nnnn*::*nn*:> fields were added to the command output.
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 Release 12.2(14)S.
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.
12.2(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 can help determine whether the router is sending or receiving IPv6 ICMP neighbor discovery messages.

Note By default, the network server sends the output from debug commands and system error messages to the console. To redirect debug output, use the logging command options within global configuration mode. Destinations include the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server. For complete information on debug commands and redirecting debug output, refer to the *Cisco IOS Debug Command Reference*.

Examples

The following example shows output for the **debug ipv6 nd** command:

```
Router# debug ipv6 nd

13:22:40:ICMPv6-ND:STALE -> DELAY:2000:0:0:3::2
13:22:45:ICMPv6-ND:DELAY -> PROBE:2000:0:0:3::2
13:22:45:ICMPv6-ND:Sending NS for 2000:0:0:3::2 on FastEthernet0/0
13:22:45:ICMPv6-ND:Received NA for 2000:0:0:3::2 on FastEthernet0/0 from 2000:0:0:3::2
13:22:45:ICMPv6-ND:PROBE -> REACH:2000:0:0:3::2
13:22:45:ICMPv6-ND:Received NS for 2000:0:0:3::1 on FastEthernet0/0 from
FE80::203:A0FF:FED6:1400
13:22:45:ICMPv6-ND:Sending NA for 2000:0:0:3::1 on FastEthernet0/0

13:23:15: ICMPv6-ND: Sending NS for FE80::1 on Ethernet0/1
13:23:16: ICMPv6-ND: DAD: FE80::1 is unique.
13:23:16: ICMPv6-ND: Sending NS for 2000::2 on Ethernet0/1
13:23:16: ICMPv6-ND: Sending NS for 3000::3 on Ethernet0/1
13:23:16: ICMPv6-ND: Sending NA for FE80::1 on Ethernet0/1
13:23:17: ICMPv6-ND: DAD: 2000::2 is unique.
13:23:53: ICMPv6-ND: Sending NA for 2000::2 on Ethernet0/1
13:23:53: ICMPv6-ND: DAD: 3000::3 is unique.
13:23:53: ICMPv6-ND: Sending NA for 3000::3 on Ethernet0/1
3d19h: ICMPv6-ND: Sending NS for FE80::2 on Ethernet0/2
3d19h: ICMPv6-ND: Received NA for FE80::2 on Ethernet0/2 from FE80::2
3d19h: ICMPv6-ND: DAD: duplicate link-local FE80::2 on Ethernet0/2,interface stalled
3d19h: %IPV6-4-DUPLICATE: Duplicate address FE80::2 on Ethernet0/2
3d19h: ICMPv6-ND: Sending NS for 3000::4 on Ethernet0/3
3d19h: ICMPv6-ND: Received NA for 3000::4 on Ethernet0/3 from 3000::4
3d19h: %IPV6-4-DUPLICATE: Duplicate address 3000::4 on Ethernet0/3
```

Table 22 describes the significant fields shown in the display.

Table 22 debug ipv6 nd Field Descriptions

Field	Description
13:22:40:	Indicates the time (hours:minutes:seconds) at which the ICMP neighbor discovery event occrred.
ICMPv6-ND	Indicates that a state change is occurring for an entry in the IPv6 neighbors cache.
STALE	Stale state. This state of an neighbor discovery cache entry used to be “reachable,” but is now is “stale” due to the entry not being used. In order to use this address, the router must go through the neighbor discovery process in order to confirm reachability.
DELAY	Delayed state. Reachability for this ND cache entry is currently being reconfirmed. While in the delay state, upper-layer protocols may inform IPv6 that they have confirmed reachability to the entry. Therefore, there is no need to send a neighbor solicitation for the entry.
PROBE	Probe state. While in the probe state, if no confirmation is received from the upper-layer protocols about the reachability of the entry, a neighbor solicitation message is sent. The entry remains in the “probe” state until a neighbor advertisement message is received in response to the neighbor solicitation message.

Table 22 debug ipv6 nd Field Descriptions (continued)

Field	Description
Sending NS for...	Sending a neighbor solicitation message. In the example output, a neighbor solicitation message is sent on Fast Ethernet interface 0/0 to determine the link-layer address of 2000:0:0:3::2 on Fast Ethernet interface 0/0.
Received NA for...	Received a neighbor advertisement message. In the example output, a neighbor advertisement message is received from the address 2000:0:0:3::2 (the second address) that includes the link-layer address of 2000:0:0:3::2 (first address) from Ethernet interface 0/0.
REACH	Reachable state. An ND cache entry in this state is considered reachable, and the corresponding link-layer address can be used without needing to perform neighbor discovery on the address.
Received NS for...	Received neighbor solicitations. In the example output, the address FE80::203:A0FF:FED6:1400 (on Fast Ethernet interface 0/0) is trying to determine the link-local address of 2000:0:0:3::1.
Sending NA for...	Sending for neighbor advertisements. In the example output, a neighbor advertisement containing the link-layer address of 2000:0:0:3::1 (an address assigned to the Fast Ethernet interface 0/0 address) was sent.
DAD: FE80::1 is unique.	Duplicate address detection processing was performed on the unicast IPv6 address (a neighbor solicitation message was not received in response to a neighbor advertisement message that contained the unicast IPv6 address) and the address is unique.
3d19h:	Indicates time (days, hours) since the last reboot of the event occurring; 3d19h: indicates the time (since the last reboot) of the event occurring was 3 days and 19 hours ago.
DAD: duplicate link-local FE80::2 on Ethernet0/2, interface stalled	Duplicate address detection processing was performed on the link-local IPv6 address (the link-local address FE80::2 is used in the example). A neighbor advertisement message was received in response to a neighbor solicitation message that contained the link-local IPv6 address. The address is not unique, and the processing of IPv6 packets is disabled on the interface.
%IPV6-4-DUPLICATE: Duplicate address...	System error message indicating the duplicate address.
Received NA for 3000::4 on Ethernet0/3 from 3000::4	Duplicate address detection processing was performed on the global IPv6 address (the global address 3000::4 is used in the example). A neighbor advertisement message was received in response to a neighbor solicitation message that contained the global IPv6 address. The address is not unique and is not used.

Related Commands

Command	Description
debug ipv6 icmp	Displays debug messages for IPv6 ICMP transactions.
show ipv6 neighbors	Displays IPv6 neighbor discovery cache information.

debug ipv6 ospf

To display debugging information for Open Shortest Path First (OSPF) for IPv6, use the **debug ipv6 ospf** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ipv6 ospf [**adj | ipsec | database-timer | flood | hello | lsa-generation | retransmission**]

no debug ipv6 ospf [**adj | ipsec | database-timer | flood | hello | lsa-generation | retransmission**]

Syntax Description

adj	(Optional) Displays adjacency information.
ipsec	(Optional) Displays the interaction between OSPF and IPSec in IPv6 networks, including creation and removal of policy definitions.
database-timer	(Optional) Displays database-timer information.
flood	(Optional) Displays flooding information.
hello	(Optional) Displays hello packet information.
l2api	(Optional) Enables layer 2 and layer 3 application program interface (API) debugging.
lsa-generation	(Optional) Displays link-state advertisement (LSA) generation information for all LSA types.
retransmission	(Optional) Displays retransmission information.

Command Default

Debugging of OSPF for IPv6 is not enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated in Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated in Cisco IOS Release 12.2(18)S.
12.3(4)T	The **ipsec** keyword was added to support OSPF for IPv6 authentication for IPSec.
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.
12.4(25)T	The **l2api** keyword was added.

Usage Guidelines

Consult Cisco technical support before using this command.

Examples

The following example displays adjacency information for OSPF for IPv6:

```
Router# debug ipv6 ospf adj
```

debug ipv6 ospf database-timer rate-limit

To display debugging information about the current wait-time used for SPF scheduling, use the **debug ipv6 ospf database-timer rate-limit** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ipv6 ospf database-timer rate-limit [*acl-number*]

no debug ipv6 ospf database-timer rate-limit

Syntax Description

acl-number	(Optional) Access list number.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

Consult Cisco technical support before using this command.

Examples

The following example shows how to turn on debugging for SPF scheduling:

```
Router# debug ipv6 ospf database-timer rate-limit
```

debug ipv6 ospf events

To display information on Open Shortest Path First (OSPF)-related events, such as designated router selection and shortest path first (SPF) calculation, use the **debug ipv6 ospf events** command in privileged EXEC command. To disable debugging output, use the **no** form of this command.

debug ipv6 ospf events

no debug ipv6 ospf events

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)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.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

Consult Cisco technical support before using this command.

Examples

The following example displays information on OSPF-related events:

```
Router# debug ipv6 ospf events
```

debug ipv6 ospf graceful-restart

To enable debugging for IPv6 graceful-restart-related events, use the **debug ipv6 ospf graceful-restart** command in privileged EXEC mode.

debug ipv6 ospf graceful-restart

Syntax Description

This command has no arguments or keywords.

Command Default

Debugging is not enabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

The **debug ipv6 ospf graceful-restart** command helps troubleshoot graceful-restart-related events on both graceful-restart-capable and graceful-restart-aware routers.

Examples

The following example enables debugging for graceful-restart-related events:

```
Router# debug ipv6 ospf graceful-restart

00:03:41: OSPFv3: GR timer started for ospf process 1 for 120 secs,
00:03:43: OSPFv3: GR  Build Grace LSA for interface Ethernet0/0
00:03:43: OSPFv3: GR Flood grace lsa on Ethernet0/0
00:03:43: OSPFv3: GR complete check for area 0 process 1
00:03:43: OSPFv3: GR wait, Ethernet0/0 in area 0 not yet complete
00:03:45: OSPFv3: GR Re-flood Grace LSA on Ethernet0/0
00:04:01: OSPFv3: GR  initial wait expired
00:04:01: OSPFv3: GR complete check for area 0 process 1
00:04:01: OSPFv3: GR wait, Ethernet0/0 in area 0 not yet complete
00:04:07: OSPFv3: GR complete check for area 0 process 1
00:04:07: OSPFv3: GR re-sync completed in area 0, process 1
00:04:07: OSPFv3: GR complete check for process 1
00:04:07: OSPFv3: process 1: GR re-sync completed for all neighbors
00:04:07: OSPFv3: scheduling rtr lsa for area 0 process 1
00:04:07: OSPFv3: Post GR, flood maxaged grace-LSA on Ethernet0/0
```

Related Commands

Command	Description
graceful-restart	Enables the OSPFv3 graceful restart feature on a graceful-restart-capable router.
graceful-restart helper	Enables the OSPFv3 graceful restart feature on a graceful-restart-aware router.
show ipv6 ospf graceful-restart	Displays OSPFv3 graceful restart information.

debug ipv6 ospf lsdb

To display database modifications for Open Shortest Path First (OSPF) for IPv6, use the **debug ipv6 ospf lsdb** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ipv6 ospf lsdb

no debug ipv6 ospf lsdb

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)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.

Usage Guidelines

Consult Cisco technical support before using this command.

Examples

The following example displays database modification information for OSPF for IPv6:

```
Router# debug ipv6 ospf lsdb
```

debug ipv6 ospf monitor

To display debugging information about the current wait-time used for shortest path first (SPF) scheduling, use the **debug ipv6 ospf monitor** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ipv6 ospf monitor

no debug ipv6 ospf monitor

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

Consult Cisco technical support before using this command.

Examples

The following example shows debugging information about SPF scheduling:

```
Router# debug ipv6 ospf monitor

Sep 27 08:29:49.319: OSPFv3: Schedule SPF in area 0
        Change in LS ID 0.0.0.0, LSA type P
*Sep 27 08:29:49.327: OSPFv3: reset throttling to 5000ms next wait-interval 10000ms
*Sep 27 08:29:49.327: OSPFv3: schedule SPF: spf_time 00:09:36.032 wait_interval 5000ms
IOU_Topvar#
*Sep 27 08:29:54.331: OSPFv3: Begin SPF at 581.036ms, process time 40ms
*Sep 27 08:29:54.331:       spf_time 00:09:36.032, wait_interval 5000ms
*Sep 27 08:29:54.331: OSPFv3: Setting next wait-interval to 10000ms
*Sep 27 08:29:54.331: OSPFv3: End SPF at 581.036ms, Total elapsed time 0ms
*Sep 27 08:29:54.331:       Schedule time 00:09:41.036, Next wait_interval 10000ms
*Sep 27 08:29:54.331:       Intra: 0ms, Inter: 0ms, External: 0ms
*Sep 27 08:29:54.331:       R: 0, N: 0
*Sep 27 08:29:54.331:       SN: 0, SA: 0, X5: 0, X7: 0
*Sep 27 08:29:54.331:       SPF suspends: 0 intra, 0 total
```

debug ipv6 ospf packet

To display information about each Open Shortest Path First (OSPF) for IPv6 packet received, use the **debug ipv6 ospf packet** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ipv6 ospf packet

no debug ipv6 ospf packet

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)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.

Usage Guidelines

Consult Cisco technical support before using this command.

Examples

The following example displays information about each OSPF for IPv6 packet received:

```
Router# debug ipv6 ospf packet
```

debug ipv6 ospf spf statistic

To display statistical information while running the shortest path first (SPF) algorithm, use the **debug ipv6 ospf spf statistic** command in privileged EXEC mode. To disable the debugging output, use the **no** form of this command.

debug ipv6 ospf spf statistic

no debug ipv6 ospf spf statistic

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)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.

Usage Guidelines

The **debug ipv6 ospf spf statistic** command displays the SPF calculation times in milliseconds, the node count, and a time stamp. Consult Cisco technical support before using this command.

Examples

The following example displays statistical information while running the SPF algorithm:

```
Router# debug ipv6 ospf spf statistics
```

Related Commands

Command	Description
debug ipv6 ospf	Displays debugging information for the OSPFv3 for IPv6 feature.
debug ipv6 ospf events	Displays information on OSPFv3-related events.
debug ipv6 ospf packet	Displays information about each OSPFv3 packet received.

debug ipv6 packet

To display debug messages for IPv6 packets, use the **debug ipv6 packet** command in privileged EXEC mode. To disable debug messages for IPv6 packets, use the **no** form of this command.

debug ipv6 packet [**access-list** *access-list-name*] [**detail**]

no debug ipv6 packet [**access-list** *access-list-name*] [**detail**]

Syntax Description

access-list *access-list-name*	(Optional) Specifies an IPv6 access list. The access list name cannot contain a space or quotation mark, or begin with a numeric
detail	(Optional) May display additional detailed information about the IPv6 packet.

Command Default

Debugging for IPv6 packets is not enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)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.
12.0(23)S	The **access-list** and **detail** keywords, and the *access-list-name* argument, were added.
12.2(13)T	The **access-list** and **detail** keywords, and the *access-list-name* argument, were added.
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.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
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 **debug ipv6 packet** command is similar to the **debug ip packet** command, except that it is IPv6-specific.

Note By default, the network server sends the output from debug commands and system error messages to the console. To redirect debug output, use the logging command options within global configuration mode. Destinations include the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server. For complete information on debug commands and redirecting debug output, refer to the *Cisco IOS Debug Command Reference*.

IPv6 debugging information includes packets received, generated, and forwarded. Fast-switched packets do not generate messages. When an IPv6 access list is specified by using the **access-list** keyword and *access-list-name* argument, only packets matching the access list permit entries are displayed.

Caution Because the **debug ipv6 packet** command generates a substantial amount of output, use it only when traffic on the IPv6 network is low, so other activity on the system is not adversely affected.

Examples

The following example shows output for the **debug ipv6 packet** command:

```
Router# debug ipv6 packet

13:25:40:IPV6:source 2000:0:0:3::1 (local)
13:25:40:      dest 2000:0:0:3::2 (FastEthernet0/0)
13:25:40:      traffic class 96, flow 0x0, len 143+195, prot 6, hops 64, originating
13:25:40:IPv6:Sending on FastEthernet0/0
13:25:40:IPV6:source 2000:0:0:3::2 (FastEthernet0/0)
13:25:40:      dest 2000:0:0:3::1
13:25:40:      traffic class 96, flow 0x0, len 60+14, prot 6, hops 64, forward to ulp
13:25:45:IPV6:source FE80::203:E4FF:FE12:CC1D (local)
13:25:45:      dest FF02::9 (Ethernet1/1)
13:25:45:      traffic class 112, flow 0x0, len 72+1428, prot 17, hops 255, originating
13:25:45:IPv6:Sending on Ethernet1/1
13:25:45:IPV6:source FE80::203:E4FF:FE12:CC00 (local)
13:25:45:      dest 2000:0:0:3::2 (FastEthernet0/0)
13:25:45:      traffic class 112, flow 0x0, len 72+8, prot 58, hops 255, originating
13:25:45:IPv6:Sending on FastEthernet0/0
13:25:45:IPV6:source 2000:0:0:3::2 (FastEthernet0/0)
13:25:45:      dest FE80::203:E4FF:FE12:CC00
13:25:45:      traffic class 112, flow 0x0, len 64+14, prot 58, hops 255, forward to ulp
13:25:45:IPV6:source FE80::203:A0FF:FED6:1400 (FastEthernet0/0)
13:25:45:      dest 2000:0:0:3::1
13:25:45:      traffic class 112, flow 0x0, len 72+14, prot 58, hops 255, forward to ulp
```

Table 23 describes the significant fields shown in the display.

Table 23 debug ipv6 packet Field Descriptions

Field	Description
IPV6:	Indicates that this is an IPv6 packet.
source 2000:0:0:3::1 (local)	The source address in the IPv6 header of the packet.
dest 2000:0:0:3::2 (FastEthernet0/0)	The destination address in the IPv6 header of the packet.
traffic class 96	The contents of the traffic class field in the IPv6 header.
flow 0x0	The contents of the flow field of the IPv6 header. The flow field is used to label sequences of packets for which special handling is necessary by IPv6 routers.
len 64+14	The length of the IPv6 packet. The length is expressed as two numbers with a plus (+) character between the numbers. The first number is the length of the IPv6 portion (IPv6 header length plus payload length). The second number is the entire datagram size minus the first number.

Table 23 debug ipv6 packet Field Descriptions (continued)

Field	Description
prot 6	The protocol field in the IPv6 header. Describes the next layer protocol that is carried by the IPv6 packet. In the example, the protocol 58 signifies that the next layer protocol is ICMPv6.
hops 64	The hops field in the IPv6 packet. This field is similar in function to the IPv4 time-to-live field.
originating	The presence of this field indicates that the packet shown was originated by the router.
Sending on FastEthernet0/0	Specifies the interface on which the packet was sent.
forward to ulp	Indicates that the packet was received by the router at the destination address and was forwarded to an upper-layer protocol (ulp) for processing.

debug ipv6 pim

To enable debugging on Protocol Independent Multicast (PIM) protocol activity, use the **debug ipv6 pim** command in privileged EXEC mode. To restore the default value, use the **no** form of this command.

debug ipv6 pim [*group-name* | *group-address* | **interface** *interface-type* | **bsr** | **group** | **neighbor**]

no debug ipv6 pim [*group-name* | *group-address* | **interface** *interface-type* | **bsr** | **group** | **neighbor**]

Syntax Description

group-name | *group-address*	(Optional) IPv6 address or name of the multicast group.
interface *interface-type*	(Optional) Displays debugging statistics about a specific interface type.
bsr	(Optional) Displays debugging statistics specific to bootstrap router (BSR) protocol operation.
group	(Optional) Displays debugging information about group-related activity.
neighbor	(Optional) Displays debugging statistics related to hello message processing and neighbor cache management.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.0(28)S	The **bsr** keyword was added.
12.2(25)S	The **bsr** keyword was added.
12.3(11)T	The **bsr** keyword was 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.
12.2(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 introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

This command helps discover whether the PIM protocol activities are working correctly.

The messages displayed by the **debug ipv6 pim** command show all PIM protocol messages, such as joins and prunes, received from or sent to other routers. Use this command in conjunction with **debug ipv6 mld** to display additional multicast activity, to learn more information about the multicast routing process, or to learn why packets are forwarded out of particular interfaces.

Examples

The following example enables debugging on PIM activity:

```
Router# debug ipv6 pim
```

Related Commands

Command	Description
debug ipv6 mld	Enables debugging on MLD protocol activity.

debug ipv6 pim df-election

To display debug messages for Protocol Independent Multicast (PIM) bidirectional designated forwarder (DF) election message processing, use the **debug ipv6 pim df-election** command in privileged EXEC mode. To disable debug messages for PIM bidirectional DF election message processing, use the **no** form of this command.

debug ipv6 pim df-election [**interface** *type number*] [**rp** *rp-name* | *rp-address*]

no debug ipv6 pim df-election [**interface** *type number*] [**rp** *rp-name* | *rp-address*]

Syntax Description

interface	(Optional) Specifies that debug messages on a specified interface will be displayed.
type number	(Optional) Interface type and number. For more information, use the question mark (?) online help function.
rp	(Optional) Specifies that debug messages on a specified Route Processor (RP) will be displayed.
rp-name	(Optional) The name of the specified RP.
rp-address	(Optional) The IPv6 address of the specified RP.

Command Default

Debugging for PIM bidirectional DF election message processing is not enabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)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.

Usage Guidelines

Use the **debug ipv6 pim df-election** command if traffic is not flowing properly when operating in PIM bidirectional mode or if the **show ipv6 pim df** and **show ipv6 pim df winner** commands do not display the expected information.

Examples

The following example shows how to enable debugging for PIM bidirectional DF election message processing on Ethernet interface 1/0 and at 200::1:

```
Route# debug ipv6 pim df-election interface ethernet 1/0 rp 200::1
```

Related Commands

Command	Description
ipv6 pim rp-address	Configures the address of a PIM RP for a particular group range.
show ipv6 pim df	Displays the DF-election state of each interface for each RP.
show ipv6 pim df winner	Displays the DF-election winner on each interface for each RP.

debug ipv6 pim limit

To enable debugging for Protocol Independent Multicast (PIM) interface limits, use the **debug ipv6 pim limit** command in privileged EXEC mode. To restore the default value, use the **no** form of this command.

debug ipv6 pim limit [*group*]

no debug ipv6 pim limit

Syntax Description

group	(Optional) Specific group to be debugged.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.

Usage Guidelines

Use the **debug ipv6 pim limit** command to display debugging information for interface limits and costs. Use the optional *group* argument to specify a particular group to debug.

Examples

The following example enables PIM interface limit debugging:

```
Router# debug ipv6 pim limit
```

Related Commands

Command	Description
ipv6 multicast limit	Configures per-interface mroute state limiters in IPv6.
ipv6 multicast limit cost	Applies a cost to mroutes that match per interface mroute state limiters in IPv6.

debug ipv6 policy

To display IPv6 policy routing packet activity, use the **debug ipv6 policy** command in user EXEC or privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ipv6 policy [*access-list-name*]

no debug ipv6 policy [*access-list-name*]

Syntax Description

access-list-name	(Optional) Name of the IPv6 access list for which to clear the match counters. Names cannot contain a space or quotation mark, or begin with a numeric.

Command Default

IPv6 policy routing packet activity is not displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)S.
12.2(33)SXI4	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SXI4.
Cisco IOS XE Release 3.2S	This command was modified. It was integrated into Cisco IOS XE Release 3.2S.

Usage Guidelines

If no access list is specified using the optional *access-list-name* argument, information about all policy-matched and policy-routed packets is displayed.

After you configure IPv6 policy routing, use the **debug ipv6 policy** command to verify that IPv6 policy-based routing (PBR) is policy-routing packets normally. Policy routing looks at various parts of the packet and then routes the packet based on certain user-defined attributes in the packet. The **debug ipv6 policy** command helps you determine what policy routing is following. It displays information about whether a packet matches the criteria, and if so, the resulting routing information for the packet.

Do not use the **debug ipv6 policy** command unless you suspect a problem with IPv6 PBR policy routing.

Examples

The following example enables IPv6 policy routing packet activity. The output for this command is self-explanatory:

```
Router# debug ipv6 policy

00:02:38:IPv6 PBR:Ethernet0/0, matched src 2003::90 dst 2001:1000::1 protocol 58
00:02:38:IPv6 PBR:set nexthop 2003:1::95, interface Ethernet1/0
00:02:38:IPv6 PBR:policy route via Ethernet1/0/2003:1::95
```

debug ipv6 pool

To enable debugging on IPv6 prefix pools, use the debug ipv6 pool command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug ipv6 pool

no debug ipv6 pool

Syntax Description

This command has no keywords or arguments.

Command Default

No debugging is active.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(13)T	This command was introduced.

Examples

The following example enables debugging for IPv6 prefix pools:

```
Router# debug ipv6 pool

2w4d: IPv6 Pool: Deleting route/prefix 2001:0DB8::/29 to Virtual-Access1 for cisco
2w4d: IPv6 Pool: Returning cached entry 2001:0DB8::/29 for cisco on Virtual-Access1 to
pool1
2w4d: IPv6 Pool: Installed route/prefix 2001:0DB8::/29 to Virtual-Access1 for cisco
```

Related Commands

Command	Description
ipv6 local pool	Configures a local IPv6 prefix pool.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.
show ipv6 local pool	Displays information about defined IPv6 prefix pools.

debug ipv6 rip

To display debug messages for IPv6 Routing Information Protocol (RIP) routing transactions, use the **debug ipv6 rip** command in privileged EXEC mode. To disable debug messages for IPv6 RIP routing transactions, use the **no** form of this command.

debug ipv6 rip [*interface-type interface-number*]

no debug ipv6 rip [*interface-type interface-number*]

Syntax Description

interface-type	(Optional) The interface type about which to display debug messages.
interface-number	(Optional) The interface number about which to display debug messages.

Command Default

IPv6 RIP debugging is not enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)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 Release 12.2(14)S.
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.
12.2(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 introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The **debug ipv6 rip** command is similar to the **debug ip rip** command, except that it is IPv6-specific.

Note By default, the network server sends the output from debug commands and system error messages to the console. To redirect debug output, use the logging command options within global configuration mode. Destinations include the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server. For complete information on debug commands and redirecting debug output, refer to the *Cisco IOS Debug Command Reference*.

Using this command without arguments enables IPv6 RIP debugging for RIP packets that are sent and received on all router interfaces. Using this command with arguments enables IPv6 RIP debugging for RIP packets that are sent and received only on the specified interface.

Caution Using this command on busy networks seriously degrades the performance of the router.

Examples

The following example shows output for the **debug ipv6 rip** command:

```
Router# debug ipv6 rip

13:09:10:RIPng:Sending multicast update on Ethernet1/1 for as1_rip
13:09:10:       src=FE80::203:E4FF:FE12:CC1D
13:09:10:       dst=FF02::9 (Ethernet1/1)
13:09:10:       sport=521, dport=521, length=32
13:09:10:       command=2, version=1, mbz=0, #rte=1
13:09:10:       tag=0, metric=1, prefix=::/0
13:09:28:RIPng:response received from FE80::202:FDFF:FE77:1E42 on Ethernet1/1 for as1_rip
13:09:28:       src=FE80::202:FDFF:FE77:1E42 (Ethernet1/1)
13:09:28:       dst=FF02::9
13:09:28:       sport=521, dport=521, length=32
13:09:28:       command=2, version=1, mbz=0, #rte=1
13:09:28:       tag=0, metric=1, prefix=2000:0:0:1:1::/80
```

The example shows two RIP packets; both are updates, known as “responses” in RIP terminology and indicated by a “command” value of 2. The first is an update sent by this router, and the second is an update received by this router. Multicast update packets are sent to all neighboring IPv6 RIP routers (all routers that are on the same links as the router sending the update, and that have IPv6 RIP enabled). An IPv6 RIP router advertises the contents of its routing table to its neighbors by periodically sending update packets over those interfaces on which IPv6 RIP is configured. An IPv6 router may also send “triggered” updates immediately following a routing table change. In this case the updates only includes the changes to the routing table. An IPv6 RIP router may solicit the contents of the routing table of a neighboring router by sending a Request (command =1) message to the router. The router will respond by sending an update (Response, command=2) containing its routing table. In the example, the received response packet could be a periodic update from the address FE80::202:FDFF:FE77:1E42 or a response to a RIP request message that was previously sent by the local router.

Table 24 describes the significant fields shown in the display.

Table 24 debug ipv6 rip Field Descriptions

Field	Description
as1_rip	The name of the RIP process that is sending or receiving the update.
src	The address from which the update was originated.
dst	The destination address for the update.
sport, dport	The source and destination ports for the update. (IPv6 RIP uses port 521, as shown in the display.)
command	The command field within the RIP packet. A value of 2 indicates that the RIP packet is a response (update); a value of 1 indicates that the RIP packet is a request.
version	The version of IPv6 RIP being used. The current version is 1.
mbz	There must be a 0 (mbz) field within the RIP packet.

Table 24 debug ipv6 rip Field Descriptions (continued)

Field	Description
#rte	Indicates the number of routing table entries (RTEs) the RIP packet contains.
tag metric prefix	The tag, metric, and prefix fields are specific to each RTE contained in the update. The tag field is intended to allow for the flagging of IPv6 RIP "internal" and "external" routes. The metric field is the distance metric from the router (sending this update) to the prefix. The prefix field is the IPv6 prefix of the destination being advertised.

Related Commands

Command	Description
debug ipv6 routing	Displays debug messages for IPv6 routing table updates and route cache updates.

debug ipv6 routing

To display debug messages for IPv6 routing table updates and route cache updates, use the **debug ipv6 routing** command in privileged EXEC mode. To disable debug messages for IPv6 routing table updates and route cache updates, use the **no** form of this command.

debug ipv6 routing

no debug ipv6 routing

Syntax Description

This command has no arguments or keywords.

Command Default

Debugging for IPv6 routing table updates and route cache updates is not enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)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 Release 12.2(14)S.
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.
12.2(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 **debug ipv6 routing** command is similar to the **debug ip routing** command, except that it is IPv6-specific.

Note By default, the network server sends the output from debug commands and system error messages to the console. To redirect debug output, use the logging command options within global configuration mode. Destinations include the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server. For complete information on debug commands and redirecting debug output, refer to the *Cisco IOS Debug Command Reference*.

Examples

The following example shows output for the **debug ipv6 routing** command:

```
Router# debug ipv6 routing

13:18:43:IPv6RT0:Add 2000:0:0:1:1::/80 to table
13:18:43:IPv6RT0:Better next-hop for 2000:0:0:1:1::/80, [120/2]
13:19:09:IPv6RT0:Add 2000:0:0:2::/64 to table
```

```
13:19:09:IPv6RT0:Better next-hop for 2000:0:0:2::/64, [20/1]
13:19:09:IPv6RT0:Add 2000:0:0:2:1::/80 to table
13:19:09:IPv6RT0:Better next-hop for 2000:0:0:2:1::/80, [20/1]
13:19:09:IPv6RT0:Add 2000:0:0:4::/64 to table
13:19:09:IPv6RT0:Better next-hop for 2000:0:0:4::/64, [20/1]
13:19:37:IPv6RT0:Add 2000:0:0:6::/64 to table
13:19:37:IPv6RT0:Better next-hop for 2000:0:0:6::/64, [20/2]
```

The **debug ipv6 routing** command displays messages whenever the routing table changes. For example, the following message indicates that a route to the prefix 2000:0:0:1:1::/80 was added to the routing table at the time specified in the message.

```
13:18:43:IPv6RT0:Add 2000:0:0:1:1::/80 to table
```

The following message indicates that the prefix 2000:0:0:2::/64 was already in the routing table; however, a received advertisement provided a lower cost path to the prefix. Therefore, the routing table was updated with the lower cost path. (The [20/1] in the example is the administrative distance [20] and metric [1] of the better path.)

```
13:19:09:IPv6RT0:Better next-hop for 2000:0:0:2::/64, [20/1]
```

Related Commands

Command	Description
debug ipv6 rip	Displays debug messages for IPv6 RIP routing transactions.

debug ipv6 snooping

To enable debugging for security snooping information in IPv6, use the **debug ipv6 snooping** command in privileged EXEC mode.

debug ipv6 snooping [**binding-table** | **classifier** | **errors** | **feature-manager** | **filter** *acl* | **ha** | **hw-api** | **interface** *interface* | **memory** | **ndp-inspection** | **policy** | **vlan** *vlanid* | **switcher** | **filter** *acl* | **interface** *interface* | *vlanid*]

no debug ipv6 snooping

Syntax Description

binding-table	(Optional) Displays information about the neighbor binding table.
classifier	(Optional) Displays information about the classifier.
errors	(Optional) Displays information about snooping security errors.
feature-manager	(Optional) Displays feature manager information.
filter *acl*	(Optional) Allows users to configure an access list to filter debugged traffic.
ha	(Optional) Displays information about high availability (HA) and stateful switchover (SSO).
hw-api	(Optional) Displays information about the hardware API.
interface *interface*	(Optional) Provides debugging information on a specified interface.
memory	(Optional) Displays information about security snooping memory.
ndp-inspection	(Optional) Displays information about Neighbor Discovery inspection.
policy	(Optional)
switcher	(Optional) Displays packets handled by the switcher.
vlanid	(Optional) Provides debugging information about a specified VLAN ID.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

The **debug ipv6 snooping** command provides debugging output for IPv6 snooping information.

Because debugging output is assigned high priority in the CPU process, you should use debug commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff.

Examples

The following example enables debugging for all IPv6 snooping information:

```
Router# debug ipv6 snooping
```

debug ipv6 snooping raguard

To enable debugging for security snooping information in the IPv6 router advertisement (RA) guard feature, use the **debug ipv6 snooping raguard** command in privileged EXEC mode.

debug ipv6 snooping raguard [*filter* | *interface* | *vlanid*]

no debug ipv6 snooping raguard

Syntax Description

filter	(Optional) Allows users to configure an access list to filter debugged traffic.
interface	(Optional) Provides debugging information on a specified interface configured with the IPv6 RA guard feature.
vlanid	(Optional) Provides debugging information about a specified VLAN ID configured with the IPv6 RA guard feature.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(54)SG	This command was introduced.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

The **debug ipv6 snooping raguard** command provides debugging output for IPv6 RA guard events and errors that may occur.

Because debugging output is assigned high priority in the CPU process, you should use debug commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Also, you should use debug commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased debug command processing overhead will affect system use.

Examples

The following example enables debugging for the IPv6 RA guard feature:

```
Router# debug ipv6 snooping raguard
```

Related Commands

Command	Description
ipv6 nd raguard	Applies the IPv6 RA guard feature.

debug ipv6 spd

To enable debugging output for the most recent Selective Packet Discard (SPD) state transition, use the **debug ipv6 spd** command in privileged EXEC mode.

debug ipv6 spd

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 **debug ipv6 spd** command enables debugging information to be reviewed for the most recent SPD state transition and any trend historical data.

Examples

The following example shows how to enable debugging for the most recent SPD state transition:

```
Router# debug ipv6 spd
```

debug ipv6 static

To enable Bidirectional Forwarding Detection for IPv6 (BFDv6) debugging, use the **debug ipv6 static** command in privileged EXEC mode.

debug ipv6 static

Command Default

Debugging is not enabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.1.0	This command was introduced.
15.1(2)T	This command was modified. It was integrated into Cisco IOS Release 15.1(2)T.

Usage Guidelines

Use the **debug ipv6 static** command to monitor BFDv6 operation.

Examples

The following example enables BFDv6 debugging:

```
Router# debug ipv6 static
```

Related Commands

Command	Description
monitor event ipv6 static	Monitors the operation of the IPv6 static and IPv6 static BFDv6 neighbors using event trace.
show ipv6 static	Displays the current contents of the IPv6 routing table.

debug isis spf-events

To display a log of significant events during an Intermediate System-to-Intermediate System (IS-IS) shortest-path first (SPF) computation, use the **debug isis spf-events** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug isis spf-events

no debug isis spf-events

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0	This command was introduced.
12.2(15)T	Support for IPv6 was added.
12.2(18)S	Support for IPv6 was added.
12.0(26)S	Support for IPv6 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.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.6	This command was introduced on Cisco ASR 1000 series routers.

Usage Guidelines

This command displays information about significant events that occur during SPF-related processing.

Examples

The following example displays significant events during an IS-IS SPF computation:

```
Router# debug isis spf-events

ISIS-Spf:  Compute L2 IPv6 SPT
ISIS-Spf: Move 0000.0000.1111.00-00 to PATHS, metric 0
ISIS-Spf: Add 0000.0000.2222.01-00 to TENT, metric 10
ISIS-Spf: Move 0000.0000.2222.01-00 to PATHS, metric 10
ISIS-Spf: considering adj to 0000.0000.2222 (Ethernet3/1) metric 10, level 2, circuit 3,
adj 3
ISIS-Spf:   (accepted)
ISIS-Spf: Add 0000.0000.2222.00-00 to TENT, metric 10
ISIS-Spf:   Next hop 0000.0000.2222 (Ethernet3/1)
ISIS-Spf: Move 0000.0000.2222.00-00 to PATHS, metric 10
ISIS-Spf: Add 0000.0000.2222.02-00 to TENT, metric 20
ISIS-Spf:   Next hop 0000.0000.2222 (Ethernet3/1)
```

```
ISIS-Spf: Move 0000.0000.2222.02-00 to PATHS, metric 20
ISIS-Spf: Add 0000.0000.3333.00-00 to TENT, metric 20
ISIS-Spf:   Next hop 0000.0000.2222 (Ethernet3/1)
ISIS-Spf: Move 0000.0000.3333.00-00 to PATHS, metric 20
```

debug nhrp

To enable Next Hop Resolution Protocol (NHRP) debugging, use the **debug nhrp** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug nhrp {**ipv4** | **ipv6**} [**cache** | **extension** | **packet** | **rate**]

no debug nhrp

Syntax Description(

ipv4	Specifies the IPv4 overlay address.
ipv6	Specifies the IPv6 overlay address.
cache	(Optional) Specifies NHRP cache operations.
extension	(Optional) Specifies NHRP extension processing.
packet	(Optional) Specifies NHRP activity.
rate	(Optional) Specifies NHRP rate limiting.

Command Default

NHRP debugging is not enabled.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following example shows NHRP debugging output for IPv6:

```
Router# debug nhrp ipv6

Aug  9 13:13:41.486: NHRP: Attempting to send packet via DEST
           - 2001:0db8:3c4d:0015:0000:0000:1a2f:3d2c/32
Aug  9 13:13:41.486: NHRP: Encapsulation succeeded.
Aug  9 13:13:41.486: NHRP: Tunnel NBMA addr 11.11.11.99
Aug  9 13:13:41.486: NHRP: Send Registration Request via Tunnel0 vrf 0, packet size: 105
Aug  9 13:13:41.486: src: 2001:0db8:3c4d:0015:0000:0000:1a2f:3d2c/32,
             dst: 2001:0db8:3c4d:0015:0000:0000:1a2f:3d2c/32
Aug  9 13:13:41.486: NHRP: 105 bytes out Tunnel0
Aug  9 13:13:41.486: NHRP: Receive Registration Reply via Tunnel0 vrf 0, packet size: 125
```

The following example shows NHRP debugging output for IPv4:

```
Router# debug nhrp ipv4

Aug  9 13:13:41.486: NHRP: Attempting to send packet via DEST 10.1.1.99
Aug  9 13:13:41.486: NHRP: Encapsulation succeeded.  Tunnel IP addr 10.11.11.99
Aug  9 13:13:41.486: NHRP: Send Registration Request via Tunnel0 vrf 0, packet size: 105
Aug  9 13:13:41.486:       src: 10.1.1.11, dst: 10.1.1.99
Aug  9 13:13:41.486: NHRP: 105 bytes out Tunnel0
Aug  9 13:13:41.486: NHRP: Receive Registration Reply via Tunnel0 vrf 0, packet size: 125
Aug  9 13:13:41.486: NHRP: netid_in = 0, to_us = 1
```

Related Commands

Command	Description
debug dmvpn	Displays DMVPN session debugging information.
debug nhrp error	Displays NHRP error level debugging information.

debug nhrp condition

To enable Next Hop Resolution Protocol (NHRP) conditional debugging, use the **debug nhrp condition** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug nhrp condition [**interface tunnel** *number* | **peer** {**nbma** {*ip-address* | *FQDN-string*} | **tunnel** {*ip-address* | *ipv6-address*}} | **vrf** *vrf-name*]

no debug nhrp condition [**interface tunnel** *number* | **peer** {**nbma** {*ip-address* | *FQDN-string*} | **tunnel** {*ip-address* | *ipv6-address*}} | **vrf** *vrf-name*]

Syntax Description

tunnel	(Optional) Specifies a tunnel.
interface	(Optional) Displays NHRP information based on a specific interface.
tunnel *number*	(Optional) Specifies the tunnel address for the NHRP peer.
peer	(Optional) Specifies an NHRP peer.
nbma	(Optional) Specifies mapping nonbroadcast multiple access (NBMA).
ip-address	(Optional) The IPv4 address for the NHRP peer.
FQDN-string	(Optional) Next hop server (NHS) fully qualified domain name (FQDN) string.
ipv6-address	(Optional) The IPv6 address for the NHRP peer. **Note** Cisco IOS XE Release 2.5 does not support the *ipv6-address* argument.
vrf *vrf-name*	(Optional) Specifies debugging information for sessions related to the specified virtual routing and forwarding (VRF) configuration.

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.

Examples

The following example shows how to enable conditional NHRP debugging for a specified NBMA address:

```
Router# debug nhrp condition peer tunnel 192.0.2.1
```

The following example shows how to enable conditional NHRP debugging for a specified FQDN string:

```
Router# debug nhrp condition peer examplehub.example1.com
```

Related Commands

Command	Description
debug dmvpn	Displays DMVPN session debugging information.
debug nhrp error	Displays NHRP error level debugging information.

debug nhrp error

To display Next Hop Resolution Protocol (NHRP) error-level debugging information, use the **debug nhrp error** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug nhrp {**ipv4** | **ipv6**} **error**

no debug nhrp {**ipv4** | **ipv6**} **error**

Syntax Description

ipv4	Specifies the IPv6 overlay network.
ipv6	Specifies the IPv6 overlay network. **Note** Cisco IOS XE Release 2.5 does not support the **ipv6** keyword.

Command Default

NHRP error-level debugging is not enabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.4(20)T	The **ipv4** and **ipv6** keywords were added.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.

Examples

The following example shows how to enable error level debugging for IPv4 NHRP:

```
Router# debug nhrp ipv4 error

NHRP errors debugging is on
```

Related Commands

Command	Description
debug dmvpn	Displays DMVPN session debugging information.
debug nhrp condition	Enables NHRP conditional debugging.

debug ntp

To display debugging messages for Network Time Protocol (NTP) features, use the **debug ntp** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ntp {**adjust** | **all** | **authentication** | **core** | **events** | **loopfilter** | **packet** | **params** | **refclock** | **select** | **sync** | **validity**}

no debug ntp {**adjust** | **all** | **authentication** | **core** | **events** | **loopfilter** | **packet** | **params** | **refclock** | **select** | **sync** | **validity**}

Syntax Description

adjust	Displays debugging information on NTP clock adjustments.
all	Displays all debugging information on NTP.
authentication	Displays debugging information on NTP authentication.
core	Displays debugging information on NTP core messages.
events	Displays debugging information on NTP events.
loopfilter	Displays debugging information on NTP loop filters.
packet	Displays debugging information on NTP packets.
params	Displays debugging information on NTP clock parameters.
refclock	Displays debugging information on NTP reference clocks.
select	Displays debugging information on NTP clock selection.
sync	Displays debugging information on NTP clock synchronization.
validity	Displays debugging information on NTP peer clock validity.

Command Default

Debugging is not enabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1	This command was introduced in a release prior to Cisco IOS Release 12.1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(20)T	Support for IPv6 and NTP version 4 was added. The **all** and **core** keywords were added. The **authentication**, **loopfilter**, **params**, **select**, **sync** and **validity** keywords were removed. The **packets** keyword was modified as **packet**.

Usage Guidelines

Starting from Cisco IOS Release 12.4(20)T, NTP version 4 is supported. In NTP version 4 the debugging options available are **adjust**, **all**, **core**, **events**, **packet**, and **refclock**. In NTP version 3 the debugging options available were **events**, **authentication**, **loopfilter**, **packets**, **params**, **select**, **sync** and **validity**.

Examples

The following example shows how to enable all debugging options for NTP:

```
Router# debug ntp all

NTP events debugging is on
NTP core messages debugging is on
NTP clock adjustments debugging is on
NTP reference clocks debugging is on
NTP packets debugging is on
```

Related Commands

Command	Description
ntp refclock	Configures an external clock source for use with NTP services.

debug ospfv3

To display debugging information for Open Shortest Path First version 3 (OSPF) for IPv4 and IPv6, use the **debug ospfv3** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ospfv3 [*process-id*] [*address-family*] [**adj** | **ipsec** | **database-timer** | **flood** | **hello** | **lsa-generation** | **retransmission**]

no debug ospfv3 [*process-id*] [*address-family*] [**adj** | **ipsec** | **database-timer** | **flood** | **hello** | **lsa-generation** | **retransmission**]

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
adj	(Optional) Displays adjacency information.
ipsec	(Optional) Displays the interaction between OSPFv3 and IPSec, including creation and removal of policy definitions.
database-timer	(Optional) Displays database-timer information.
flood	(Optional) Displays flooding information.
hello	(Optional) Displays hello packet information.
l2api	(Optional) Enables layer 2 and layer 3 application program interface (API) debugging.
lsa-generation	(Optional) Displays link-state advertisement (LSA) generation information for all LSA types.
retransmission	(Optional) Displays retransmission information.

Command Default

Debugging of OSPFv3 is not enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

Consult Cisco technical support before using this command.

Examples

The following example displays adjacency information for OSPFv3:

```
Router# debug ospfv3 adj
```

debug ospfv3 database-timer rate-limit

To display debugging information about the current wait-time used for shortest path first (SPF) scheduling, use the **debug ospfv3 database-timer rate-limit** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ospfv3 [*process-id*] [*address-family*] **database-timer rate-limit** [*acl-number*]

no debug ospfv3 [*process-id*] [*address-family*] **database-timer rate-limit**

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
acl-number	(Optional) Access list number.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

Consult Cisco technical support before using this command.

Examples

The following example shows how to turn on debugging for SPF scheduling in OSPFv3 process 1:

```
Router# debug ospfv3 1 database-timer rate-limit
```

debug ospfv3 events

To display information on Open Shortest Path First version 3 (OSPFv3)-related events, such as designated router selection and shortest path first (SPF) calculation, use the **debug ospfv3 events** command in privileged EXEC command. To disable debugging output, use the **no** form of this command.

debug ospfv3 [*process-id*] [*address-family*] **events**

no debug ipv6 ospfv3 [*process-id*] [*address-family*] **events**

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

Consult Cisco technical support before using this command.

Examples

The following example displays information on OSPFv3-related events:

```
Router# debug ospfv3 events
```

debug ospfv3 lsdb

To display database modifications for Open Shortest Path First version 3 (OSPFv3), use the **debug ospfv3 lsdb** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ospfv3 [*process-id*] [*address-family*] **lsdb**

no debug ospfv3 [*process-id*] [*address-family*] **lsdb**

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

Consult Cisco technical support before using this command.

Examples

The following example displays database modification information for OSPFv3:

```
Router# debug ospfv3 lsdb
```

debug ospfv3 packet

To display information about each Open Shortest Path First version 3 (OSPFv3) packet received, use the **debug ospfv3 packet** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ospfv3 [*process-id*] [*address-family*] **packet**

no debug ospfv3 [*process-id*] [*address-family*] **packet**

SyntaxDescription

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

Consult Cisco technical support before using this command.

Examples

The following example displays information about each OSPFv3 packet received:

```
Router# debug ospfv3 packet
```

debug ospfv3 spf statistic

To display statistical information while running the shortest path first (SPF) algorithm, use the **debug ospfv3 spf statistic** command in privileged EXEC mode. To disable the debugging output, use the **no** form of this command.

debug ospfv3 [*address-family*] **spf statistic**

no debug ospfv3 [*address-family*] **spf statistic**

Syntax Description

address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

The **debug ospfv3 spf statistic** command displays the SPF calculation times in milliseconds, the node count, and a time stamp. Consult Cisco technical support before using this command.

Examples

The following example displays statistical information while running the SPF algorithm:

```
Router# debug ospfv3 spf statistics
```

Related Commands

Command	Description
debug ospfv3	Displays debugging information for the OSPFv3 feature.
debug ospfv3 events	Displays information on OSPFv3-related events.
debug ospfv3 packet	Displays information about each OSPFv3 packet received.

debug ppp unique address

To display debugging information about duplicate addresses received from RADIUS, use the **debug ppp unique address** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ipv6 policy

no debug ipv6 policy

Syntax Description

This command has no arguments or keywords.

Command Default

Information about duplicate addresses received from RADIUS is not displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines

The **debug ppp unique address** command enables you to view debugging information about duplicate addresses received from RADIUS.

Examples

The following example enables debugging output about duplicate addresses received from RADIUS:

```
Router# debug ppp unique address
```

default (IPv6 OSPF)

To return a parameter to its default value, use the **default** command in router configuration mode.

default [**area** | **auto-cost** | **default-information** | **default-metric** | **discard-route** | **distance** | **distribute-list** | **ignore** | **log-adjacency-changes** | **maximum-paths** | **passive-interface** | **redistribute** | **router-id** | **summary-prefix** | **timers**]

Syntax Description

area	(Optional) Open Shortest Path First (OSPF) for IPv6 area parameters.
auto-cost	(Optional) OSPF interface cost according to bandwidth.
default-information	(Optional) Distributes default information.
default-metric	(Optional) Metric for a redistributed route.
discard-route	(Optional) Enables or disables discard-route installation.
distance	(Optional) Administrative distance.
distribute-list	(Optional) Filter networks in routing updates.
ignore	(Optional) Ignores a specific event.
log-adjacency-changes	(Optional) Log changes in the adjacency state.
maximum-paths	(Optional) Forwards packets over multiple paths.
passive-interface	(Optional) Suppresses routing updates on an interface.
redistribute	(Optional) Redistributes IPv6 prefixes from another routing protocol.
router-id	(Optional) Router ID for the specified routing process.
summary-prefix	(Optional) OSPF summary prefix.
timers	(Optional) OSPF timers.

Command Default

This command is disabled by default.

Command Modes

Router 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.

Usage Guidelines

The command is removed if it is disabled by default.

Examples

In the following example, OSPF for IPv6 area parameters are reset to the default values:

```
default timers spf
```

default (OSPFv3)

To return an Open Shortest Path First version 3 (OSPFv3) parameter to its default value, use the **default** command in OSPFv3 router configuration mode, IPv6 address family configuration mode, or IPv4 address family configuration mode.

default {**area** *area-ID* [**range** *ipv6-prefix* | **virtual-link** *router-id*]} [**default-information originate** [**always** | **metric** | **metric-type** | **route-map**] | **distance** | **distribute-list** *prefix-list prefix-list-name* {**in** | **out**} [*interface*] | **maximum-paths** *paths* | **redistribute** *protocol* | **summary-prefix** *ipv6-prefix*]

Syntax Description

area	OSPFv3 area parameters.
area-ID	Area ID associated with the OSPFv3 interface.
range	Summarizes routes that match the address or address mask on border routers only.
ipv6-prefix	An IPv6 address.
virtual-link	Defines a virtual link and its parameters.s
router-id	Router ID associated with the virtual-link neighbor.
default-information originate	(Optional) Distribution of default route information.
always	(Optional) Always provides the default route information.
metric	(Optional) Provides the OSPFv3 default metric.
metric-type	(Optional) Provides the OSPFv3 metric type for default routes.
route-map	(Optional) Provides the route-map reference.
distance	(Optional) Provides the administrative distance.
distribute-list	(Optional) Filter networks in routing updates.
prefix-list *prefix-list-name*	Filters connections based on an IPv6 prefix list.
in	Filters incoming routing updates.
out	Filters outgoing routing updates.
interface	(Optional) Filters incoming or outgoing routing updates on a specified interface.
maximum-paths	(Optional) Forwards packets over multiple paths.
paths	Maximum number of paths. The range is from 1 through 32.
redistribute	(Optional) Redistributes IPv6 prefixes from another routing protocol.
protocol	The routing protocol from which IPv6 prefixes are redistributed.
summary-prefix	(Optional) OSPFv3 summary prefix.

Command Default

This command is disabled by default.

Command Modes

OSPFv3 router configuration mode (config-router)
IPv6 address family configuration (config-router-af)
IPv4 address family configuration (config-router-af)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

Use the **default** command in OSPFv3 router configuration mode to reset OSPFv3 parameters for an IPv4 OSPFv3 process.

Use the **default** command in IPv6 or IPv4 address family configuration mode to reset OSPFv3 parameters for an IPv6 or an IPv4 process.

Examples

In the following example, OSPFv3 parameters are reset to the default value for area 1 in IPv6 address family configuration mode:

```
Router(config-router)# address-family ipv6 unicast
Router(config-router-af)# default area 1
```

Related Commands

Command	Description
address-family ipv4	Enters IPv4 address family configuration mode for OSPFv3.
address-family ipv6	Enters IPv6 address family configuration mode for OSPFv3.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

default-information originate (IPv6 IS-IS)

To inject an IPv6 default route into an Intermediate System-to-Intermediate System (IS-IS) IPv6 routing domain, use the **default-information originate** command in address family configuration mode. To disable this feature, use the **no** form of this command.

default-information originate [**route-map** *map-name*]

no default-information originate [**route-map** *map-name*]

Syntax Description

route-map *map-name*	(Optional) Route map should be used to advertise the default route conditionally. The *map-name* argument identifies a configured route map.

Command Default

This feature is disabled.

Command Modes

Address family configuration

Command History

Release	Modification
12.2(8)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 Release 12.2(14)S.
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.
12.2(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 2.4	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The **default-information originate** (IPv6 IS-IS) command is similar to the **default-information originate** (IS-IS) command, except that it is IPv6-specific.

If a router configured with this command has an IPv6 route to ::/0 in the routing table, IS-IS will originate an advertisement for ::/0 in its link-state packets (LSPs).

Without a route map, the default is advertised only in Level 2 LSPs. For Level 1 routing, there is another mechanism to find the default route, which is for the router to look for the closest Level 1 or Level 2 router. The closest Level 1 or Level 2 router can be found by looking at the attached bit (ATT) in Level 1 LSPs.

A route map can be used for two purposes:

- Make the router generate default in its Level 1 LSPs.

- Advertise ::/0 conditionally.

With a **match ipv6 address** *standard-access-list* command, you can specify one or more IPv6 routes that must exist before the router will advertise ::/0.

Examples

The following example shows the IPv6 default route (::/0) being advertised with all other routes in router updates:

```
Router(config)# router isis area01
Router(config-router)# address-family ipv6
Router(config-router-af)# default-information originate
```

Related Commands

Command	Description
address-family ipv6 (IS-IS)	Specifies the IPv6 address family and places the router in address family configuration mode.
match ipv6 address	Distributes IPv6 routes that have a prefix permitted by a prefix list.
show isis database	Displays the IS-IS link-state database.

default-information originate (OSPFv3)

To generate a default external route into an Open Shortest Path First version 3 (OSPFv3) for a routing domain, use the **default-information originate** command in IPv6 or IPv4 address family configuration mode. To disable this feature, use the **no** form of this command.

default-information originate [**always** | **metric** *metric-value* | **metric-type** *type-value* | **route-map** *map-name*]

no default-information originate [**always** | **metric** *metric-value* | **metric-type** *type-value* | **route-map** *map-name*]

Syntax Description

always	(Optional) Always advertises the default route regardless of whether the software has a default route.
metric *metric-value*	(Optional) Metric used for generating the default route. If you omit a value and do not specify a value using the **default-metric** router configuration command, the default metric value is 10. The default metric value range is from 0 to 16777214.
metric-type *type-value*	(Optional) External link type associated with the default route advertised into the OSPF for IPv6 routing domain. It can be one of the following values: **1**—Type 1 external route **2**—Type 2 external route The default is type 2 external route.
route-map *map-name*	(Optional) Routing process will generate the default route if the route map is satisfied.

Command Default

This command is disabled by default.

Command Modes

IPv6 address family configuration (config-router-af)
IPv4 address family configuration (config-router-af)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

Whenever you use the **redistribute** or the **default-information** command to redistribute routes into an OSPFv3 routing domain, the Cisco IOS software automatically becomes an Autonomous System Boundary Router (ASBR). However, an ASBR does not, by default, generate a *default route* into the OSPF for IPv6 routing domain. The software still must have a default route for itself before it generates one, except when you have specified the **always** keyword.

When you use this command for the OSPFv3 process, the default network must reside in the routing table, and you must satisfy the **route-map** *map-name* keyword and argument. Use the **default-information originate always route-map** *map-name* form of the command when you do not want the dependency on the default network in the routing table.

Examples

The following example specifies a metric of 100 for the default route redistributed into the OSPFv3 routing domain, an external metric type of type 2, and the default route to be always advertised:

```
Router(config-router-af)# default-information originate always metric 100 metric-type 2
```

default-metric (EIGRP)

To set metrics for Enhanced Interior Gateway Routing Protocol (EIGRP), use the **default-metric** command in router configuration mode or address-family topology configuration mode. To remove the metric value and restore the default state, use the **no** form of this command.

default-metric *bandwidth delay reliability loading mtu*

no default-metric *bandwidth delay reliability loading mtu*

Syntax Description

bandwidth	Minimum bandwidth of the route in kilobytes per second. It can be from 1 to 4294967295.
delay	Route delay in tens of microseconds. It can be 1 or any positive number that is a multiple of 39.1 nanoseconds.
reliability	Likelihood of successful packet transmission expressed as a number from 0 through 255. The value 255 means 100 percent reliability; 0 means no reliability.
loading	Effective bandwidth of the route expressed as a number from 1 to 255 (255 is 100 percent loading).
mtu	The smallest allowed value for the maximum transmission unit (MTU), expressed in bytes. It can be from 1 to 65535.

Command Default

Only connected routes can be redistributed without a default metric. The metric of redistributed connected routes is set to 0.

Command Modes

Router configuration (config-router)
Address-family topology configuration (config-router-af-topology)

Command History

Release	Modification
10.0	This command was introduced.
12.0(22)S	Address family support was added.
12.2(15)T	Address family support was added.
12.2(18)S	Address family support was added.
12.4(6)T	Support for IPv6 was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
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.
15.0(1)M	This command was modified. Address-family topology configuration mode was added. This command must be entered in address-family topology configuration mode when EIGRP is configured with a named router configuration.

Release	Modification
12.2(33)SRE	This command was modified. Address-family topology configuration mode was added. This command must be entered in address-family topology configuration mode when EIGRP is configured with a named router configuration.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

You must use a default metric to redistribute a protocol into EIGRP, unless you use the **redistribute** command.

Metric defaults have been carefully set to work for a wide variety of networks. Take great care when changing these values.

Default metrics are supported only when you are redistributing from EIGRP or static routes.

Examples

The following example shows how the redistributed Routing Information Protocol (RIP) metrics are translated into EIGRP metrics with values as follows: bandwidth = 1000, delay = 100, reliability = 250, loading = 100, and MTU = 1500:

```
Router(config)# router eigrp 109
Router(config-router)# network 172.16.0.0
Router(config-router)# redistribute rip
Router(config-router)# default-metric 1000 100 250 100 1500
```

The following example shows how the redistributed EIGRP service family 6473 metrics are translated into EIGRP metric with values as follows: bandwidth = 1000, delay = 100, reliability = 250, loading = 100, and MTU = 1500.

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# af-interface default
Router(config-router-af-interface)# no shutdown
Router(config-router-af-interface)# exit
Router(config-router-af)# topology base
Router(config-router-af-topology)# default-metric 1000 100 250 100 1500
```

Related Commands

Command	Description
address-family (EIGRP)	Enters address-family configuration mode to configure an EIGRP routing instance.
af-interface	Enters address-family interface configuration mode to configure interface-specific EIGRP commands.
ipv6 router eigrp	Configures the EIGRP IPv6 routing process.
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.
redistribute (IPv6)	Redistributes IPv6 routes from one routing domain into another routing domain.

Command	Description
router eigrp	Configures the EIGRP address-family process.
topology (EIGRP)	Configures an EIGRP process to route IP traffic under the specified topology instance and enters router address-family topology configuration mode.

default-metric (OSPFv3)

To set default metric values for IPv4 and IPv6 routes redistributed into the Open Shortest Path First version 3 (OSPFv3) routing protocol, use the **default-metric** command in OSPFv3 router configuration mode, IPv6 address family configuration mode, or IPv4 address family configuration mode. To return to the default state, use the **no** form of this command.

default-metric *metric-value*

no default-metric *metric-value*

Syntax Description

metric-value	Default metric value appropriate for the specified routing protocol. The range is from 1 to 4294967295.

Command Default

Built-in, automatic metric translations, as appropriate for each routing protocol.

Command Modes

OSPFv3 router configuration mode (config-router)
IPv6 address family configuration (config-router-af)
IPv4 address family configuration (config-router-af)

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.
15.1(3)S	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.
Cisco IOS XE Release 3.4S	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.
15.2(1)T	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.

Usage Guidelines

The **default-metric** command is used in conjunction with the **redistribute** router configuration command to cause the current routing protocol to use the same metric value for all redistributed routes. A default metric helps solve the problem of redistributing routes with incompatible metrics. Whenever metrics do not convert, using a default metric provides a reasonable substitute and enables the redistribution to proceed.

Finer control over the metrics of redistributed routes can be gained by using the options to the **redistribute** command, including route maps.

Examples

The following example shows how to enter IPv6 AF and configure OSPFv3 routing protocol redistributing routes from the OSPFv3 process named process1. All the redistributed routes are advertised with a metric of 10.

```
router ospfv3 100
 address-family ipv6 unicast
 default-metric 10
 redistribute ospfv3 process1
```

The following example shows an OSPFv3 routing protocol redistributing routes from the OSPFv3 process named process1. All the redistributed routes are advertised with a metric of 10.

```
ipv6 router ospf 100
 default-metric 10
 redistribute ospfv3 process1
```

Related Commands

Command	Description
redistribute (OSPFv3)	Redistributes IPv6 and IPv4 routes from one routing domain into another routing domain.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

deny (IPv6)

To set deny conditions for an IPv6 access list, use the **deny** command in IPv6 access list configuration mode. To remove the deny conditions, use the **no** form of this command.

deny *protocol* {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix*/*prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*] [**undetermined-transport**]

no deny *protocol* {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix*/*prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*] [**undetermined-transport**]

Internet Control Message Protocol

deny icmp {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix*/*prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [*icmp-type* [*icmp-code*] | *icmp-message*] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]

Transmission Control Protocol

deny tcp {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix*/*prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [**ack**] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**established**] [**fin**] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**neq** {*port* | *protocol*}] [**psh**] [**range** {*port* | *protocol*}] [**routing**] [**routing-type** *routing-number*] [**rst**] [**sequence** *value*] [**syn**] [**time-range** *name*] [**urg**]

User Datagram Protocol

deny udp {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix*/*prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**neq** {*port* | *protocol*}] [**range** {*port* | *protocol*}] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]

Syntax Description

protocol	Name or number of an Internet protocol. It can be one of the keywords **ahp**, **esp**, **icmp**, **ipv6**, **pcp**, **sctp**, **tcp**, or **udp**, or an integer in the range from 0 to 255 representing an IPv6 protocol number.
source-ipv6-prefix/*prefix-length*	The source IPv6 network or class of networks about which to set deny conditions. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
any	An abbreviation for the IPv6 prefix ::/0.
host *source-ipv6-address*	The source IPv6 host address about which to set deny conditions. This *source-ipv6-address* argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
operator [*port-number*]	(Optional) Specifies an operand that compares the source or destination ports of the specified protocol. Operands are **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range** (inclusive range). If the operator is positioned after the *source-ipv6-prefix*/*prefix-length* argument, it must match the source port. If the operator is positioned after the *destination-ipv6-prefix*/*prefix-length* argument, it must match the destination port. The **range** operator requires two port numbers. All other operators require one port number. The optional *port-number* argument is a decimal number or the name of a TCP or UDP port. A port number is a number from 0 to 65535. TCP port names can be used only when filtering TCP. UDP port names can be used only when filtering UDP.
destination-ipv6-prefix/*prefix-length*	The destination IPv6 network or class of networks about which to set deny conditions. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
host *destination-ipv6-address*	The destination IPv6 host address about which to set deny conditions. This *destination-ipv6-address* argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
auth	Allows matching traffic against the presence of the authentication header in combination with the specified protocol; that is, TCP or UDP.
dest-option-type	(Optional) Matches IPv6 packets against the destination option extension header within each IPv6 packet header.
doh-number	(Optional) Integer in the range from 0 to 255 representing an IPv6 destination option extension header.
doh-type	(Optional) Destination option header types. The possible destination option header type and its corresponding *doh-number* value are home-address—201.
dscp *value*	(Optional) Matches a differentiated services code point value against the traffic class value in the Traffic Class field of each IPv6 packet header. The acceptable range is from 0 to 63.

flow-label *value*	(Optional) Matches a flow label value against the flow label value in the Flow Label field of each IPv6 packet header. The acceptable range is from 0 to 1048575.
fragments	(Optional) Matches non-initial fragmented packets where the fragment extension header contains a non-zero fragment offset. The **fragments** keyword is an option only if the *operator* [*port-number*] arguments are not specified.
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 name and sequence number, whether the packet was 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 denied in the prior 5-minute interval.
log-input	(Optional) Provides the same function as the **log** keyword, except that the logging message also includes the input interface.
mobility	(Optional) Extension header type. Allows matching of any IPv6 packet including a mobility header, regardless of the value of the mobility-header-type field within that header.
mobility-type	(Optional) Mobility header type. Either the *mh-number* or *mh-type* argument must be used with this keyword.
mh-number	(Optional) Integer in the range from 0 to 255 representing an IPv6 mobility header type.
mh-type	(Optional) Name of a mobility header type. Possible mobility header types and their corresponding *mh-number* value are as follows: • 0—bind-refresh • 1—hoti • 2—coti • 3—hot • 4—cot • 5—bind-update • 6—bind-acknowledgment • 7—bind-error
routing	(Optional) Matches source-routed packets against the routing extension header within each IPv6 packet header.
routing-type	(Optional) Allows routing headers with a value in the type field to be matched independently. The *routing-number* argument must be used with this keyword.
routing-number	Integer in the range from 0 to 255 representing an IPv6 routing header type. Possible routing header types and their corresponding *routing-number* value are as follows: • 0—Standard IPv6 routing header • 2—Mobile IPv6 routing header

sequence *value*	(Optional) Specifies the sequence number for the access list statement. The acceptable range is from 1 to 4294967295.
time-range *name*	(Optional) Specifies the time range that applies to the deny statement. The name of the time range and its restrictions are specified by the **time-range** and **absolute** or **periodic** commands, respectively.
undetermined-transport	(Optional) Matches packets from a source for which the Layer 4 protocol cannot be determined. The **undetermined-transport** keyword is an option only if the *operator* [*port-number*] arguments are not specified.
icmp-type	(Optional) Specifies an ICMP message type for filtering ICMP packets. ICMP packets can be filtered by ICMP message type. The ICMP message type can be a number from 0 to 255, some of which include the following predefined strings and their corresponding numeric values: • 144—dhaad-request • 145—dhaad-reply • 146—mpd-solicitation • 147—mpd-advertisement
icmp-code	(Optional) Specifies an ICMP message code for filtering ICMP packets. 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) Specifies an ICMP message name for filtering ICMP packets. ICMP packets can be filtered by an ICMP message name or ICMP message type and code. The possible names are listed in the "Usage Guidelines" section.
ack	(Optional) For the TCP protocol only: acknowledgment (ACK) bit set.
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.
fin	(Optional) For the TCP protocol only: Fin bit set; no more data from sender.
neq {*port* | *protocol*}	(Optional) Matches only packets that are not on a given port number.
psh	(Optional) For the TCP protocol only: Push function bit set.
range {*port* | *protocol*}	(Optional) Matches only packets in the range of port numbers.
rst	(Optional) For the TCP protocol only: Reset bit set.
syn	(Optional) For the TCP protocol only: Synchronize bit set.
urg	(Optional) For the TCP protocol only: Urgent pointer bit set.

Command Default No IPv6 access list is defined.

Command Modes IPv6 access list configuration

Command History

Release	Modification
12.0(23)S	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.
12.4(2)T	The *icmp-type* argument was enhanced. The **dest-option-type**, **mobility**, **mobility-type**, and **routing-type** keywords were added. The *doh-number*, *doh-type*, *mh-number*, *mh-type*, and *routing-number* arguments 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.
12.2(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 introduced on Cisco ASR 1000 Series Routers.
12.4(20)T	The **auth** keyword was added.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

The **deny** (IPv6) command is similar to the **deny** (IP) command, except that it is IPv6-specific.

Use the **deny** (IPv6) command following the **ipv6 access-list** command to define the conditions under which a packet passes the access list or to define the access list as a reflexive access list.

Specifying IPv6 for the *protocol* argument matches against the IPv6 header of the packet.

By 1default, the first statement in an access list is number 10, and the subsequent statements are numbered in increments of 10.

You can add **permit**, **deny**, **remark**, or **evaluate** statements to an existing access list without retyping the entire list. To add a new statement anywhere other than at the end of the list, create a new statement with an appropriate entry number that falls between two existing entry numbers to indicate where it belongs.

In Cisco IOS Release 12.2(2)T or later releases, 12.0(21)ST, and 12.0(22)S, IPv6 access control lists (ACLs) are defined and their deny and permit conditions are set by using the **ipv6 access-list** command with the **deny** and **permit** keywords in global configuration mode. In Cisco IOS Release 12.0(23)S or later releases, IPv6 ACLs are defined by using the **ipv6 access-list** command in global configuration mode and their permit and deny conditions are set by using the **deny** and **permit** commands in IPv6 access list configuration mode. Refer to the **ipv6 access-list** command for more information on defining IPv6 ACLs.

Note In Cisco IOS Release 12.0(23)S or later releases, every IPv6 ACL has implicit **permit icmp any any nd-na**, **permit icmp any any nd-ns**, and **deny ipv6 any any** statements as its last match conditions. (The former two match conditions allow for ICMPv6 neighbor discovery.) An IPv6 ACL must contain at least one entry for the implicit **deny ipv6 any any** statement to take effect.

The IPv6 neighbor discovery process makes use of the IPv6 network layer service; therefore, by default, IPv6 ACLs implicitly allow IPv6 neighbor discovery packets to be sent and received on an interface. In IPv4, the Address Resolution Protocol (ARP), which is equivalent to the IPv6 neighbor discovery process, makes use of a separate data link layer protocol; therefore, by default, IPv4 ACLs implicitly allow ARP packets to be sent and received on an interface.

Both the *source-ipv6-prefix*/*prefix-length* and *destination-ipv6-prefix*/*prefix-length* arguments are used for traffic filtering (the source prefix filters traffic based upon the traffic source; the destination prefix filters traffic based upon the traffic destination).

Note IPv6 prefix lists, not access lists, should be used for filtering routing protocol prefixes.

The **fragments** keyword is an option only if the *operator* [*port-number*] arguments are not specified.

The **undetermined-transport** keyword is an option only if the *operator* [*port-number*] arguments are not specified.

The following is a list of ICMP message names:

- beyond-scope
- destination-unreachable
- echo-reply
- echo-request
- header
- hop-limit
- mld-query
- mld-reduction
- mld-report
- nd-na
- nd-ns
- next-header
- no-admin
- no-route
- packet-too-big
- parameter-option
- parameter-problem
- port-unreachable
- reassembly-timeout
- renum-command
- renum-result
- renum-seq-number
- router-advertisement
- router-renumbering
- router-solicitation
- time-exceeded
- unreachable

Examples

The following example configures the IPv6 access list named toCISCO and applies the access list to outbound traffic on Ethernet interface 0. Specifically, the first deny entry in the list keeps all packets that have a destination TCP port number greater than 5000 from exiting out of Ethernet interface 0. The second deny entry in the list keeps all packets that have a source UDP port number less than 5000 from exiting out of Ethernet interface 0. The second deny also logs all matches to the console. The first permit entry in the list permits all ICMP packets to exit out of Ethernet interface 0. The second permit entry in the list permits all other traffic to exit out of Ethernet interface 0. The second permit entry is necessary because an implicit deny all condition is at the end of each IPv6 access list.

```
ipv6 access-list toCISCO
 deny tcp any any gt 5000
 deny ::/0 lt 5000 ::/0 log
 permit icmp any any
 permit any any

interface ethernet 0
 ipv6 traffic-filter toCISCO out
```

The following example shows how to allow TCP or UDP parsing although an IPsec AH is present:

```
IPv6 access list example1
    deny tcp host 2001::1 any log sequence 5
    permit tcp any any auth sequence 10
    permit udp any any auth sequence 20
```

Related Commands

Command	Description
ipv6 access-list	Defines an IPv6 access list and enters IPv6 access list configuration mode.
ipv6 traffic-filter	Filters incoming or outgoing IPv6 traffic on an interface.
permit (IPv6)	Sets permit conditions for an IPv6 access list.
show ipv6 access-list	Displays the contents of all current IPv6 access lists.

destination-pattern

To specify either the prefix or the full E.164 telephone number to be used for a dial peer, use the **destination-pattern** command in dial peer configuration mode. To disable the configured prefix or telephone number, use the **no** form of this command.

destination-pattern [**+**]*string*[**T**]

no destination-pattern [**+**]*string*[**T**]

Syntax Description

+	(Optional) Character that indicates an E.164 standard number.
string	Series of digits that specify a pattern for the E.164 or private dialing plan telephone number. Valid entries are the digits 0 through 9, the letters A through D, and the following special characters: • The asterisk (*) and pound sign (#) that appear on standard touch-tone dial pads. • Comma (,), which inserts a pause between digits. • Period (.), which matches any entered digit (this character is used as a wildcard). • Percent sign (%), which indicates that the preceding digit occurred zero or more times; similar to the wildcard usage. • Plus sign (+), which indicates that the preceding digit occurred one or more times. **Note** The plus sign used as part of a digit string is different from the plus sign that can be used preceding a digit string to indicate that the string is an E.164 standard number. • Circumflex (^), which indicates a match to the beginning of the string. • Dollar sign ($), which matches the null string at the end of the input string. • Backslash symbol (\), which is followed by a single character, and matches that character. Can be used with a single character with no other significance (matching that character). • Question mark (?), which indicates that the preceding digit occurred zero or one time. • Brackets ([ ]), which indicate a range. A range is a sequence of characters enclosed in the brackets; only numeric characters from 0 to 9 are allowed in the range. • Parentheses (( )), which indicate a pattern and are the same as the regular expression rule.
T	(Optional) Control character that indicates that the **destination-pattern** value is a variable-length dial string. Using this control character enables the router to wait until all digits are received before routing the call.

Command Default The command is enabled with a null string.

Command Modes Dial peer configuration (config-dial-peer)

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
11.3(1)MA	This command was implemented on the Cisco MC3810.
12.0(4)XJ	This command was modified for store-and-forward fax.
12.1(1)	The command was integrated into Cisco IOS Release 12.1(1).
12.0(7)XR	This command was implemented on the Cisco AS5300 and modified to support the plus sign, percent sign, question mark, brackets, and parentheses symbols in the dial string.
12.0(7)XK	This command was modified. Support for the plus sign, percent sign, question mark, brackets, and parentheses in the dial string was added to the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T and implemented on the Cisco 1750, Cisco 7200 series, and Cisco 7500 series. The modifications for the Cisco MC3810 in Cisco IOS Release12.0(7)XK are not supported in this release.
12.1(2)T	The modifications made in Cisco IOS Release 12.0(7)XK for the Cisco MC3810 were integrated into Cisco IOS Release 12.1(2)T.
12.2(8)T	This command was implemented on the Cisco 1751, Cisco 2600 series and Cisco 3600 series, Cisco 3725, and Cisco 3745.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T and implemented on the Cisco 2600XM, the Cisco ICS7750, and the Cisco VG200.
12.4(22)T	Support for IPv6 was added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines Use the **destination-pattern** command to define the E.164 telephone number for a dial peer.

The pattern you configure is used to match dialed digits to a dial peer. The dial peer is then used to complete the call. When a router receives voice data, it compares the called number (the full E.164 telephone number) in the packet header with the number configured as the destination pattern for the voice-telephony peer. The router then strips out the left-justified numbers that correspond to the destination pattern. If you have configured a prefix, the prefix is prepended to the remaining numbers, creating a dial string that the router then dials. If all numbers in the destination pattern are stripped out, the user receives a dial tone.

There are areas in the world (for example, certain European countries) where valid telephone numbers can vary in length. Use the optional control character **T** to indicate that a particular **destination-pattern** value is a variable-length dial string. In this case, the system does not match the dialed numbers until the interdigit timeout value has expired.

Note Cisco IOS software does not verify the validity of the E.164 telephone number; it accepts any series of digits as a valid number.

Examples

The following example shows configuration of the E.164 telephone number 555-0179 for a dial peer:

```
dial-peer voice 10 pots
 destination-pattern +5550179
```

The following example shows configuration of a destination pattern in which the pattern “43” is repeated multiple times preceding the digits “555”:

```
dial-peer voice 1 voip
 destination-pattern 555(43)+
```

The following example shows configuration of a destination pattern in which the preceding digit pattern is repeated multiple times:

```
dial-peer voice 2 voip
 destination-pattern 555%
```

The following example shows configuration of a destination pattern in which the possible numeric values are between 5550109 and 5550199:

```
dial-peer voice 3 vofr
 destination-pattern 55501[0-9]9
```

The following example shows configuration of a destination pattern in which the possible numeric values are between 5550439, 5553439, 5555439, 5557439, and 5559439:

```
dial-peer voice 4 voatm
 destination-pattern 555[03579]439
```

The following example shows configuration of a destination pattern in which the digit-by-digit matching is prevented and the entire string is received:

```
dial-peer voice 2 voip
 destination-pattern 555T
```

Related Commands

Command	Description
answer-address	Specifies the full E.164 telephone number to be used to identify the dial peer of an incoming call.
dial-peer terminator	Designates a special character to be used as a terminator for variable-length dialed numbers.
incoming called-number (dial peer)	Specifies a digit string that can be matched by an incoming call to associate that call with a dial peer.
prefix	Specifies the prefix of the dialed digits for a dial peer.
timeouts interdigit	Configures the interdigit timeout value for a specified voice port.

device-role

To specify the role of the device attached to the port, use the **device-role** command in Neighbor Discovery (ND) inspection policy configuration mode or Router Advertisement (RA) guard policy configuration mode.

device-role {**host** | **monitor** | **router**}

Syntax Description

host	Sets the role of the device to host.
monitor	Sets the role of the device to monitor.
router	Sets the role of the device to router.

Command Default

The device role is host.

Command Modes

ND inspection policy configuration (config-nd-inspection)
RA guard policy configuration (config-ra-guard)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

The **device-role** command specifies the role of the device attached to the port. By default, the device role is host, and therefore all the inbound router advertisement and redirect messages are blocked. If the device role is enabled using the **router** keyword, all messages (router solicitation [RS], RA, or redirect) are allowed on this port.

When the **router** or **monitor** keywords are used, the multicast RS are bridged on the port, regardless of whether limited broadcast is enabled. However, the **monitor** keyword does not allow inbound RA or redirect messages. When the **monitor** keyword is used, devices that need these messages will receive them.

Examples

The following example defines an NDP policy name as policy1, places the router in ND inspection policy configuration mode, and configures the device as the host:

```
Router(config)# ipv6 nd inspection policy policy1
Router(config-nd-inspection)# device-role host
```

The following example defines an RA guard policy name as raguard1, places the router in RA guard policy configuration mode, and configures the device as the host:

```
Router(config)# ipv6 nd raguard policy raguard1
Router(config-ra-guard)# device-role host
```

Related Commands

Command	Description
ipv6 nd inspection policy	Defines the ND inspection policy name and enters ND inspection policy configuration mode.
ipv6 nd raguard policy	Defines the RA guard policy name and enter RA guard policy configuration mode.

dial-peer voice

To define a particular dial peer, to specify the method of voice encapsulation, and to enter dial peer configuration mode, use the **dial-peer voice** command in global configuration mode. To delete a defined dial peer, use the **no** form of this command.

Cisco 1750 and Cisco 1751 Modular Access Routers

dial-peer voice *tag* {**pots** | **vofr** | **voip system**}

no dial-peer voice *tag* {**pots** | **vofr** | **voip system**}

Cisco 2600 Series, Cisco 2600XM, Cisco 3600 Series, Cisco 3700 Series, Cisco 7204VXR and Cisco 7206VXR

dial-peer voice *tag* {**pots** | **voatm** | **vofr** | **voip system**}

no dial-peer voice *tag* {**pots** | **voatm** | **vofr** | **voip system**}

Cisco 7200 Series

dial-peer voice *tag* **vofr**

no dial-peer voice *tag* **vofr**

Cisco AS5300

dial-peer voice *tag* {**mmoip** | **pots** | **vofr** | **voip system**}

no dial-peer voice *tag* {**mmoip** | **pots** | **vofr** | **voip system**}

Syntax Description

tag	Digits that define a particular dial peer. Range is from 1 to 2147483647.
pots	Indicates that this is a POTS peer that uses VoIP encapsulation on the IP backbone.
vofr	Specifies that this is a Voice over Frame Relay (VoFR) dial peer that uses FRF.11 encapsulation on the Frame Relay backbone network.
voip	Indicates that this is a VoIP peer that uses voice encapsulation on the POTS network.
system	Indicates that this is a system that uses VoIP.
voatm	Specifies that this is a Voice over ATM (VoATM) dial peer that uses real-time ATM adaptation layer 5 (AAL5) voice encapsulation on the ATM backbone network.
mmoip	Indicates that this is a multimedia mail peer that uses IP encapsulation on the IP backbone.

Command Default

No dial peer is defined.
No method of voice encapsulation is specified.

Command Modes Global configuration (config)

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
11.3(1)MA	This command was implemented on the Cisco MC3810, with support for the **pots**, **voatm**, **vofr**, and **vohdlc** keywords.
12.0(3)T	This command was implemented on the Cisco AS5300, with support for the **pots** and **voip** keywords.
12.0(3)XG	The **vofr** keyword was added for the Cisco 2600 series and Cisco 3600 series.
12.0(4)T	The **vofr** keyword was added for the Cisco 7200 series.
12.0(4)XJ	The **mmoip** keyword was added for the Cisco AS5300. The **dial-peer voice** command was implemented for store-and-forward fax.
12.0(7)XK	The **voip** keyword was added for the Cisco MC3810, and the **voatm** keyword was added for the Cisco 3600 series. Support for the **vohdlc** keyword on the Cisco MC3810 was removed.
12.1(1)	The **mmoip** keyword addition in Cisco IOS Release 12.0(4)XJ was integrated into Cisco IOS Release 12.1(1). The **dial-peer voice** implementation for store-and-forward fax was integrated into Cisco IOS Release 12.1(1).
12.1(2)T	The keyword changes in Cisco IOS Release 12.0(7)XK were integrated into Cisco IOS Release 12.1(2)T.
12.1(5)T	This command was implemented on the Cisco AS5300 and integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(2)XN	Support for enhanced Media Gateway Control Protocol (MGCP) voice gateway interoperability was added to Cisco CallManager Version 3.1 for the Cisco 2600 series, Cisco 3600 series, and Cisco VG200.
12.2(8)T	This command was implemented on the Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and Cisco CallManager Version 3.2. This command was implemented on the Cisco IAD2420 series.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T and implemented on the Cisco 2600XM, Cisco ICS7750, and Cisco VG200.
12.4(22)T	Support for IPv6 was added.

Usage Guidelines Use the **dial-peer voice** global configuration command to switch to dial peer configuration mode from global configuration mode and to define a particular dial peer. Use the **exit** command to exit dial peer configuration mode and return to global configuration mode.

A newly created dial peer remains defined and active until you delete it with the **no** form of the **dial-peer voice** command. To disable a dial peer, use the **no shutdown** command in dial peer configuration mode.

In store-and-forward fax on the Cisco AS5300, the POTS dial peer defines the inbound faxing line characteristics from the sending fax device to the receiving Cisco AS5300 and the outbound line characteristics from the sending Cisco AS5300 to the receiving fax device. The Multimedia Mail over Internet Protocol (MMoIP) dial peer defines the inbound faxing line characteristics from the Cisco AS5300 to the receiving Simple Mail Transfer Protocol (SMTP) mail server. This command works with both on-ramp and off-ramp store-and-forward fax functions.

Note On the Cisco AS5300, MMoIP is available only if you have modem ISDN channel aggregation (MICA) technologies modems.

Examples

The following example shows how to access dial peer configuration mode and configure a POTS peer identified as dial peer 10 and an MMoIP dial peer identified as dial peer 20:

```
dial-peer voice 10 pots
dial-peer voice 20 mmoip
```

The following example deletes the MMoIP peer identified as dial peer 20:

```
no dial-peer voice 20 mmoip
```

The following example shows how the **dial-peer voice** command is used to configure the extended echo canceller. In this instance, **pots** indicates that this is a POTS peer using VoIP encapsulation on the IP backbone, and it uses the unique numeric identifier tag 133001.

```
Router(config)# dial-peer voice 133001 pots
```

Related Commands

Command	Description
codec (dial-peer)	Specifies the voice coder rate of speech for a VoFR dial peer.
destination-pattern	Specifies the prefix, the full E.164 telephone number, or an ISDN directory number to be used for a dial peer.
dtmf-relay (Voice over Frame Relay)	Enables the generation of FRF.11 Annex A frames for a dial peer.
preference	Indicates the preferred order of a dial peer within a rotary hunt group.
sequence-numbers	Enables the generation of sequence numbers in each frame generated by the DSP for VoFR applications.
session protocol	Establishes a session protocol for calls between the local and remote routers via the packet network.
session target	Specifies a network-specific address for a specified dial peer or destination gatekeeper.
shutdown	Changes the administrative state of the selected dial peer from up to down.

dialer-group

To control access by configuring an interface to belong to a specific dialing group, use the **dialer-group** command in interface configuration mode. To remove an interface from the specified dialer access group, use the **no** form of this command.

dialer-group *group-number*

no dialer-group

Syntax Description

group-number	Number of the dialer access group to which the specific interface belongs. This access group is defined with the **dialer-list** command. Acceptable values are nonzero, positive integers between 1 and 10.

Defaults

No access is predefined.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(13)T	Support for IPv6 was added.
Cisco IOS XE Release 2.5	This command was updated. It was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

An interface can be associated with a single dialer access group only; multiple **dialer-group** assignment is not allowed. A second dialer access group assignment will override the first. A dialer access group is defined with the **dialer-group** command. The **dialer-list** command associates an access list with a dialer access group.

Packets that match the dialer group specified trigger a connection request.

Examples

The following example specifies dialer access group number 1.

The destination address of the packet is evaluated against the access list specified in the associated **dialer-list** command. If it passes, either a call is initiated (if no connection has already been established) or the idle timer is reset (if a call is currently connected).

```
interface async 1
 dialer-group 1
access-list 101 deny igrp 0.0.0.0 255.255.255.255 255.255.255.255 0.0.0.0
access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
dialer-list 1 protocol ip list 101
```

Related Commands

Command	Description
dialer-list protocol (Dial)	Defines a DDR dialer list to control dialing by protocol or by a combination of protocol and an access list.

dialer-list protocol

To define a dial-on-demand routing (DDR) dialer list for dialing by protocol or by a combination of a protocol and a previously defined access list, use the **dialer-list protocol** command in global configuration mode. To delete a dialer list, use the **no** form of this command.

dialer-list *dialer-group* **protocol** *protocol-name* {**permit** | **deny** | **list** *access-list-number* | *access-group*}

no dialer-list *dialer-group* [**protocol** *protocol-name* [**list** *access-list-number* | *access-group*]]

Syntax Description

dialer-group	Number of a dialer access group identified in any **dialer-group** interface configuration command.
protocol-name	One of the following protocol keywords: **appletalk**, **bridge**, **clns**, **clns_es**, **clns_is**, **decnet**, **decnet_router-L1**, **decnet_router-L2**, **decnet_node**, **ip**, **ipx**, **ipv6**, **vines**, or **xns**.
permit	Permits access to an entire protocol.
deny	Denies access to an entire protocol.
list	Specifies that an access list will be used for defining a granularity finer than an entire protocol.
access-list-number	Access list numbers specified in any DECnet, Banyan VINES, IP, Novell IPX, or XNS standard or extended access lists, including Novell IPX extended service access point (SAP) access lists and bridging types, and IPv6 access lists. See Table 25 for the supported access list types and numbers.
access-group	Filter list name used in the **clns filter-set** and **clns access-group** commands.

Command Default

No dialer lists are defined.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
10.3	The following keyword and arguments were added: • **list** • *access-list-number* and *access-group*
12.2(2)T	The **ipv6** keyword was added.
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 Release 12.2(14)S.
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.

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.
Cisco IOS XE Release 2.5	This command was updated. It was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

The various **no** forms of this command have the following effects:

- The **no dialer-list 1** command deletes all lists configured with list 1, regardless of the keyword previously used (**permit**, **deny**, **protocol**, or **list**).
- The **no dialer-list 1 protocol** *protocol-name* command deletes all lists configured with list 1 and **protocol** *protocol-name*.
- The **no dialer-list 1 protocol** *protocol-name* **list** *access-list-number* command deletes the specified list.

The **dialer-list protocol** command permits or denies access to an entire protocol. The **dialer-list protocol list** command provides a finer permission granularity and also supports protocols that were not previously supported.

The **dialer-list protocol list** command applies protocol access lists to dialer access groups to control dialing using DDR. The dialer access groups are defined with the **dialer-group** command.

Table 25 lists the access list types and number range that the **dialer-list protocol list** command supports. The table does not include International Organization for Standardization (ISO) Connectionless Network Services (CLNS) or IPv6 because those protocols use filter names instead of predefined access list numbers.

Table 25 dialer-list protocol Command Supported Access List Types and Number Range

Access List Type	Access List Number Range (Decimal)
AppleTalk	600 to 699
Banyan VINES (standard)	1 to 100
Banyan VINES (extended)	101 to 200
DECnet	300 to 399
IP (standard)	1 to 99
IP (extended)	100 to 199
Novell IPX (standard)	800 to 899
Novell IPX (extended)	900 to 999
Transparent Bridging	200 to 299
XNS	500 to 599

Examples

Dialing occurs when an interesting packet (one that matches access list specifications) needs to be output on an interface. Using the standard access list method, packets can be classified as interesting or uninteresting. In the following example, Integrated Gateway Routing Protocol (IGRP) TCP/IP routing protocol updates are not classified as interesting and do not initiate calls:

```
access-list 101 deny igrp 0.0.0.0 255.255.255.255 255.255.255.255 0.0.0.0
```

The following example classifies all other IP packets as interesting and permits them to initiate calls:

```
access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
```

Then the following command places list 101 into dialer access group 1:

```
dialer-list 1 protocol ip list 101
```

In the following example, DECnet access lists allow any DECnet packets with source area 10 and destination area 20 to trigger calls:

```
access-list 301 permit 10.0 0.1023 10.0 0.1023
access-list 301 permit 10.0 0.1023 20.0 0.1023
```

Then the following command places access list 301 into dialer access group 1:

```
dialer-list 1 protocol decnet list 301
```

In the following example, both IP and VINES access lists are defined. The IP access lists define IGRP packets as uninteresting, but permits all other IP packets to trigger calls. The VINES access lists do not allow Routing Table Protocol (RTP) routing updates to trigger calls, but allow any other data packets to trigger calls.

```
access-list 101 deny igrp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
!
vines access-list 107 deny RTP 00000000:0000 FFFFFFFF:FFFF 00000000:0000 FFFFFFFF:FFFF
vines access-list 107 permit IP 00000000:0000 FFFFFFFF:FFFF 00000000:0000 FFFFFFFF:FFFF
```

Then the following two commands place the IP and VINES access lists into dialer access group 1:

```
dialer-list 1 protocol ip list 101
dialer-list 1 protocol vines list 107
```

In the following example, a CLNS filter is defined and then the filter is placed in dialer access group 1:

```
clns filter-set ddrline permit 47.0004.0001....
!
dialer-list 1 protocol clns list ddrline
```

The following example configures an IPv6 access list named list2 and places the access list in dialer access group 1:

```
ipv6 access-list list2 deny fec0:0:0:2::/64 any
ipv6 access-list list2 permit any any
!
dialer-list 1 protocol ipv6 list list2
```

Related Commands

Command	Description
access-list	Configures the access list mechanism for filtering frames by protocol type or vendor code.
clns filter-set	Builds a list of CLNS address templates with associated permit and deny conditions for use in CLNS filter expressions.
dialer-group	Controls access by configuring an interface to belong to a specific dialing group.

Command	Description
ipv6 access-list	Defines an IPv6 access list and sets deny or permit conditions for the defined access list.
vines access-list	Creates a VINES access list.

discard-route (IPv6)

To reinstall either an external or internal discard route that was previously removed, use the **discard-route** command in router configuration mode. To remove either an external or internal discard route, use the **no** form of this command.

discard-route [**external** | **internal**]

no discard-route [**external** | **internal**]

Syntax Description

external	(Optional) Reinstalls the discard route entry for redistributed summarized routes on an Autonomous System Boundary Router (ASBR).
internal	(Optional) Reinstalls the discard-route entry for summarized internal routes on the Area Border Router (ABR).

Command Default

External and internal discard route entries are installed.

Command Modes

Router 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.

Usage Guidelines

External and internal discard route entries are installed in routing tables by default. During route summarization, routing loops may occur when data is sent to a nonexisting network that appears to be a part of the summary, and the router performing the summarization has a less specific route (pointing back to the sending router) for this network in its routing table. To prevent the routing loop, a discard route entry is installed in the routing table of the ABR or ASBR.

If for any reason you do not want to use the external or internal discard route, remove the discard route by entering the **no discard-route** command with either the **external** or **internal** keyword.

Examples

The following display shows the discard route functionality installed by default. When external or internal routes are summarized, a summary route to Null0 will appear in the router output from the **show ipv6 route** command. See the router output lines that appear in bold font:

```
Router# show ipv6 route

IPv6 Routing Table - 7 entries
Codes:C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
O   2001::/32 [110/0]
     via ::, Null0
C   2001:0:11::/64 [0/0]
     via ::, Ethernet0/0
L   2001:0:11:0:A8BB:CCFF:FE00:6600/128 [0/0]
     via ::, Ethernet0/0
C   2001:1:1::/64 [0/0]
     via ::, Ethernet1/0
L   2001:1:1:0:A8BB:CCFF:FE00:6601/128 [0/0]
     via ::, Ethernet1/0
L   FE80::/10 [0/0]
     via ::, Null0
L   FF00::/8 [0/0]
     via ::, Null0

Router# show ipv6 route ospf

IPv6 Routing Table - 7 entries
Codes:C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
O   2001::/32 [110/0]
     via ::, Null0
```

When the **no discard-route** command with the **internal** keyword is entered, notice the following route change, indicated by the router output lines that appear in bold font:

```
Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ipv6 router ospf 1
Router(config-router)# no discard-route internal
Router(config-router)# end

Router# show ipv6 route ospf

IPv6 Routing Table - 6 entries
Codes:C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
```

Next, the **no discard-route** command with the **external** keyword is entered to remove the external discard route entry:

```
Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
Router(config-router)# no discard-route external
Router(config-router)# end
```

The following router output from the **show running-config** command confirms that both the external and internal discard routes have been removed from the routing table. See the router output lines that appear in bold font:

```
Router# show running-config

Building configuration...

Current configuration :2490 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
logging snmp-authfail
logging buffered 20480 debugging
logging console warnings
!
clock timezone PST -8
clock summer-time PDT recurring
no aaa new-model
ip subnet-zero
no ip domain lookup
!
!
ip audit po max-events 100
ipv6 unicast-routing
no ftp-server write-enable
!
.
.
.
interface Ethernet0/0
 no ip address
 ipv6 address 2001:0:11::/64 eui-64
 ipv6 enable
 ipv6 ospf 1 area 0
 no cdp enable
!
interface Ethernet1/0
 no ip address
 ipv6 address 2001:1:1::/64 eui-64
 ipv6 enable
 ipv6 ospf 1 area 1
 no cdp enable
 .
 .
 .
```

```
ipv6 router ospf 1
 router-id 2.0.0.1
 log-adjacency-changes
 no discard-route external
 no discard-route internal
 area 0 range 2001::/32
 redistribute rip 1
!
```

Related Commands

Command	Description
show ipv6 route	Displays the current contents of the IPv6 routing table.
show running config	Displays the contents of the currently running configuration file or the configuration for a specific interface, or map class information.

distance (IPv6)

To configure an administrative distance for Intermediate System-to-Intermediate System (IS-IS), Routing Information Protocol (RIP), or Open Shortest Path First (OSPF) IPv6 routes inserted into the IPv6 routing table, use the **distance** command in address family configuration or router configuration mode. To return the administrative distance to its default setting, use the **no** form of this command.

distance [**ospf** {**external** | **inter-area** | **intra-area**}] *distance*

no distance [**ospf** {**external** | **inter-area** | **intra-area**}] *distance*

Syntax Description

ospf	(Optional) Administrative distance for OSPF for IPv6 routes.
external	External type 5 and type 7 routes for OSPF for IPv6 routes.
inter-area	Inter-area routes for OSPF for IPv6 routes.
intra-area	Intra-area routes for OSPF for IPv6 routes.
distance	The administrative distance. An integer from 10 to 254. (The values 0 to 9 are reserved for internal use. Routes with a distance value of 255 are not installed in the routing table.)

Command Default

IS-IS: 115
RIP: 120
OSPF for IPv6: 110

Command Modes

Address family configuration
Router configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was implemented on the Cisco 12000 series Internet routers, and support for IS-IS was added.
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 Release 12.2(14)S.
12.2(15)T	OSPF for IPv6 information was added. The **external**, **inter-area**, and **intra-area** keywords 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.
12.2(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 2.4	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The **distance** (IPv6) command is similar to the **distance** (IP) command, except that it is IPv6-specific.

If two processes attempt to insert the same route into the same routing table, the one with the lower administrative distance takes precedence.

An administrative distance is an integer from 10 to 254. In general, the higher the value, the lower the trust rating. An administrative distance of 255 means the routing information source cannot be trusted at all and should be ignored. Distance values are subjective; there is no quantitative method for choosing the values.

Examples

The following example configures an administrative distance of 190 for the IPv6 IS-IS routing process named area01:

```
Router(config)# router isis area01
Router(config-router)# address-family ipv6
Router(config-router-af)# distance 190
```

The following example configures an administrative distance of 200 for the IPv6 RIP routing process named cisco:

```
Router(config)# ipv6 router rip cisco
Router(config-router)# distance 200
```

The following example configures an administrative distance of 200 for external type 5 and type 7 routes for OSPF for IPv6:

```
Router(config)# ipv6 router ospf
Router(config-router)# distance ospf external 200
```

distance (IPv6 EIGRP)

To allow the use of two administrative distances—internal and external—that could be a better route to a node, use the **distance** command in router configuration mode. To reset these values to their defaults, use the **no** form of this command.

distance *internal-distance external-distance*

no distance

Syntax Description

internal-distance	Administrative distance for Enhanced Internal Gateway Routing Protocol (EIGRP) for IPv6 internal routes. Internal routes are those that are learned from another entity within the same autonomous system. The distance can be a value from 1 to 255.
external-distance	Administrative distance for EIGRP for IPv6 external routes. External routes are those for which the best path is learned from a neighbor external to the autonomous system. The distance can be a value from 1 to 255.

Command Default

internal-distance: 90
external-distance: 170

Command Modes

Router configuration

Command History

Release	Modification
12.4(6)T	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.

Usage Guidelines

An administrative distance is a rating of the trustworthiness of a routing information source, such as an individual router or a group of routers. Numerically, an administrative distance is an integer from 0 to 255. In general, the higher the value, the lower the trust rating. An administrative distance of 255 means the routing information source cannot be trusted at all and should be ignored.

Use the **distance** command if another protocol is known to be able to provide a better route to a node than was actually learned via external EIGRP for IPv6, or if some internal routes should be preferred by EIGRP for IPv6.

Table 26 lists the default administrative distances.

Table 26 Default Administrative Distances

Route Source	Default Distance
Connected interface	0
Static route	1

Table 26 Default Administrative Distances (continued)

Route Source	Default Distance
EIGRP summary route	5
External Border Gateway Protocol (BGP)	20
Internal EIGRP	90
Open Shortest Path First (OSPF)	110
Intermediate System-to-Intermediate System (IS-IS)	115
Routing Information Protocol (RIP)	120
Exterior Gateway Protocol (EGP)	140
EIGRP external route	170
Internal BGP	200
Unknown	255

Examples

The following example sets the internal distance to 95 and the external distance to 165:

```
distance 95 165
```

distance (IPv6 Mobile)

To define an administrative distance for network mobility (NEMO) routes, use the **distance** command in router configuration mode. To return the administrative distance to its default distance definition, use the **no** form of this command.

distance [*mobile-distance*]

no distance

Syntax Description

mobile-distance	(Optional) Defines the mobile route, which is the default route for IPv6 over the roaming interface. The mobile default distance is 3.

Command Default

If no distances are configured, the default distances are automatically used.

Command Modes

Router configuration (config-router)

Command History

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

Usage Guidelines

The Mobile IPv6 NEMO router maintains the following type of route:

- Mobile route—Default route for IPv6 over the roaming interface

An administrative distance is a rating of the trustworthiness of a routing information source, such as an individual router or a group of routers. Numerically, an administrative distance is an integer from 0 to 255. In general, the higher the value, the lower the trust rating. An administrative distance of 255 means the routing information source cannot be trusted at all and should be ignored.

Examples

The following example defines the administrative distance for the mobile route as 10:

```
Router(config-router)# distance 10
```

Related Commands

Command	Description
ipv6 router nemo	Enables the NEMO routing process on the home agent and places the router in router configuration mode.

distance (OSPFv3)

To configure an administrative distance for Open Shortest Path First version 3 (OSPFv3) routes inserted into the routing table, use the **distance** command in IPv6 or IPv4 address family configuration mode. To return the administrative distance to its default setting, use the **no** form of this command.

distance *distance*

no distance *distance*

Syntax Description

distance	The administrative distance. An integer from 10 to 254. (The values 0 to 9 are reserved for internal use. Routes with a distance value of 255 are not installed in the routing table.)

Command Default

Administrative distance is 110.

Command Modes

IPv6 address family configuration (config-router-af)
IPv4 address family configuration (config-router-af)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

If two processes attempt to insert the same route into the same routing table, the one with the lower administrative distance takes precedence.

An administrative distance is an integer from 10 to 254. In general, the higher the value, the lower the trust rating. An administrative distance of 255 means the routing information source cannot be trusted at all and should be ignored. Distance values are subjective; there is no quantitative method for choosing the values.

Examples

The following example configures an administrative distance of 200 for OSPFv3 in an IPv6 address family:

```
Router(config-router)# address-family ipv6 unicast
Router(config-router-af)# distance 200
```

Related Commands

Command	Description
address-family ipv4	Enters IPv4 address family configuration mode for OSPFv3.
address-family ipv6	Enters IPv6 address family configuration mode for OSPFv3.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

distance bgp (IPv6)

To allow the use of external, internal, and local administrative distances that could be a better route than other external, internal, or local routes to a node, use the **distance bgp** command in address family configuration mode. To return to the default values, use the **no** form of this command

distance bgp *external-distance internal-distance local-distance*

no distance bgp

Syntax Description

external-distance	Administrative distance for Border Gateway Protocol (BGP) external routes. External routes are routes for which the best path is learned from a neighbor external to the autonomous system. Acceptable values are from 1 to 255. The default is 20. Routes with a distance of 255 are not installed in the routing table.
internal-distance	Administrative distance for BGP internal routes. Internal routes are those routes that are learned from another BGP entity within the same autonomous system. Acceptable values are from 1 to 255. The default is 200. Routes with a distance of 255 are not installed in the routing table.
local-distance	Administrative distance for BGP local routes. Local routes are those networks listed with a **network** router configuration command, often as back doors, for that router or for networks that are being redistributed from another process. Acceptable values are from 1 to 255. The default is 200. Routes with a distance of 255 are not installed in the routing table.

Command Default

external-distance: 20
internal-distance: 200
local-distance: 200

Command Modes

Address family configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
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.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
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

The **distance bgp** (IPv6) command is similar to the **distance bgp** command, except that it is IPv6-specific. Settings configured by the **distance bgp** (IPv6) command will override the default IPv6 distance settings. IPv6 BGP is not influenced by the distance settings configured in IPv4 BGP router mode.

An administrative distance is a rating of the trustworthiness of a routing information source, such as an individual router or a group of routers. Numerically, an administrative distance is a positive integer from 1 to 255. In general, the higher the value, the lower the trust rating. An administrative distance of 255 means the routing information source cannot be trusted at all and should be ignored. Distance values are subjective; there is no quantitative method for choosing the values.

Use this command if another protocol is known to be able to provide a better route to a node than was actually learned via external BGP (eBGP), or if some internal routes should be preferred by BGP.

For IPv6 multicast BGP (MBGP) distance, the distance assigned is used in reverse path forwarding (RPF) lookup. Use the **show ipv6 rpf** command to display the distance assigned.

Caution Changing the administrative distance of BGP internal routes is considered dangerous to the system and is not recommended. One problem that can arise is the accumulation of routing table inconsistencies, which can break routing.

Examples

In the following address family configuration mode example, internal routes are known to be preferable to those learned through Interior Gateway Protocol (IGP), so the IPv6 BGP administrative distance values are set accordingly:

```
router bgp 65001
 neighbor 2001:0DB8::1 remote-as 65002
 address-family ipv6
 distance bgp 20 20 200
 neighbor 2001:0DB8::1 activate
 exit-address-family
```

Related Commands

Command	Description
show ipv6 rpf	Displays RPF information for a given unicast host address and prefix.

distribute-list prefix-list (IPv6 EIGRP)

To apply a prefix list to Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 routing updates that are received or sent on an interface, use the **distribute-list prefix-list** command in router configuration mode. To remove the prefix list, use the **no** form of this command.

distribute-list prefix-list *list-name*

no distribute-list prefix-list *list-name*

Syntax Description

list-name	Name of a prefix list. The list defines which EIGRP for IPv6 networks are to be accepted in incoming routing updates and which networks are to be advertised in outgoing routing updates, based upon matching the network prefix to the prefixes in the list.

Command Default

Prefix lists are not applied to EIGRP for IPv6 routing updates.

Command Modes

Router configuration

Command History

Release	Modification
12.4(6)T	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.

Usage Guidelines

The prefix list is applied to routing updates received or sent on all interfaces.

Examples

The following example applies prefix list list1 to routes received and sent on all interfaces:

```
Router(config)# ipv6 router eigrp 1
Router(config-router)# distribute-list prefix-list list1
```

Related Commands

Command	Description
ipv6 prefix-list	Creates an entry in an IPv6 prefix list.
show ipv6 prefix-list	Displays information about an IPv6 prefix list or prefix list entries.

distribute-list prefix-list (IPv6 OSPF)

To apply a prefix list to Open Shortest Path First (OSPF) for IPv6 routing updates that are received or sent on an interface, use the **distribute-list prefix-list** command in router configuration mode. To remove the prefix list, use the **no** form of this command.

distribute-list prefix-list *list-name* {**in** [*interface-type interface-number*] | **out** *routing-process* [*as-number*]}

no distribute-list prefix-list *list-name* {**in** [*interface-type interface-number*] | **out** *routing-process* [*as-number*]}

Syntax Description

list-name	Name of a prefix list. The list defines which OSPF for IPv6 networks are to be accepted in incoming routing updates and which networks are to be advertised in outgoing routing updates, based upon matching the network prefix to the prefixes in the list.
in	Applies the prefix list to incoming routing updates on the specified interface.
interface-type interface-number	(Optional) Interface type and number. For more information, use the question mark (**?**) online help function.
out	Restricts which prefixes OSPF for IPv6 will identify to the other protocol.
routing-process	Name of a specific routing process. Valid entries for this value are **bgp, connected, eigrp**, **isis, ospf, rip,** or **static**.
as-number	(Optional) Autonomous system number, required for use with Border Gateway Protocol (BGP) and Routing Information Protocol (RIP).

Command Default

Prefix lists are not applied to OSPF for IPv6 routing updates.

Command Modes

Router 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.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Aggregation Service Routers.
12.2(33) SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 2.6	This command was modified. The **eigrp** and **ospf** keywords were added for the *routing process* argument.
15.1(2)T	This command was modified. The **eigrp** and **ospf** keywords were added for the *routing process* argument.

Usage Guidelines

If no interface is specified when the **in** keyword is used, the prefix list is applied to routing updates received on all interfaces.

Examples

The following example applies prefix list PL1 to routes received on Ethernet interface 0/0, and applies prefix list PL2 to advertised routes that came from process bgp 65:

```
Router(config)# ipv6 router ospf 1
Router(config-router)# distribute-list prefix-list PL1 in Ethernet0/0
Router(config-router)# distribute-list prefix-list PL2 out bgp 65
```

Related Commands

Command	Description
ipv6 prefix-list	Creates an entry in an IPv6 prefix list.
show ipv6 prefix-list	Displays information about an IPv6 prefix list or prefix list entries.

distribute-list prefix-list (IPv6 RIP)

To apply a prefix list to IPv6 Routing Information Protocol (RIP) routing updates that are received or sent on an interface, use the **distribute-list prefix-list** command in router configuration mode. To remove the prefix list, use the **no** form of this command.

distribute-list prefix-list *listname* {**in** | **out**} [*interface-type interface-number*]

no distribute-list prefix-list *listname*

Syntax Description

listname	Name of a prefix list. The list defines which IPv6 RIP networks are to be accepted in incoming routing updates and which networks are to be advertised in outgoing routing updates, based upon matching the network prefix to the prefixes in the list.
in	Applies the prefix list to incoming routing updates on the specified interface.
out	Applies the prefix list to outgoing routing updates on the specified interface.
interface-type	(Optional) The specified interface type. For supported interface types, use the question mark (?) online help function.
interface-number	(Optional) The specified interface number.

Command Default

Prefix lists are not applied to IPv6 RIP routing updates.

Command Modes

Router configuration

Command History

Release	Modification
12.2(2)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 Release 12.2(14)S.
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.
12.2(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 no interface is specified, the prefix list is applied to all interfaces.

Examples

The following example applies the prefix list named cisco to IPv6 RIP routing updates that are received on Ethernet interface 0/0:

```
Router(config)# ipv6 router rip cisco
```

```
Router(config-rtr-rip)# distribute-list prefix-list cisco in ethernet 0/0
```

Related Commands

Command	Description
ipv6 prefix-list	Creates an entry in an IPv6 prefix list.
show ipv6 prefix-list	Displays information about an IPv6 prefix list or prefix list entries.

dns-server (IPv6)

To specify the Domain Name System (DNS) IPv6 servers available to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **dns-server** command in DHCP for IPv6 pool configuration mode. To remove the DNS server list, use the **no** form of this command.

dns-server *ipv6-address*

no dns-server *ipv6-address*

Syntax Description

ipv6-address	The IPv6 address of a DNS server. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

Command Default

When a DHCP for IPv6 pool is first created, no DNS IPv6 servers are configured.

Command Modes

DHCP for IPv6 pool configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

Multiple Domain Name System (DNS) server addresses can be configured by issuing this command multiple times. New addresses will not overwrite old addresses.

Examples

The following example specifies the DNS IPv6 servers available:

```
dns-server 2001:0DB8:3000:3000::42
```

Related Commands

Command	Description
domain-name	Configures a domain name for a DHCP for IPv6 client.
ipv6 dhcp pool	Configures a DHCP for IPv6 configuration information pool and enters DHCP for IPv6 pool configuration mode.

domain-name (IPv6)

To configure a domain name for a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) client, use the **domain-name** command in DHCPv6 pool configuration mode. To return to the default for this command, use the **no** form of this command.

domain-name *domain-name*

no domain-name

Syntax Description

domain-name	Default domain name used to complete unqualified hostnames. **Note** Do not include the initial period that separates an unqualified name from the domain name.

Command Default

No default domain name is defined for the DNS view.

Command Modes

DHCPv6 pool configuration mode (config-dhcp)

Command History

Release	Modification
12.4(9)T	This command was introduced.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

Use the **domain-name** command in IPv6 configure a domain name for a DHCPv6 client.

Examples

The following example configures a domain name for a DHCPv6 client:

```
Router(config)# ipv6 dhcp pool pool1
Router(cfg-dns-view)# domain-name domainv6
```

drop-unsecure

To drop messages with no or invalid options or an invalid signature, use the **drop-unsecure** command in Neighbor Discovery (ND) inspection policy configuration mode. To disable this function, use the **no** form of this command.

drop-unsecure

no drop-unsecure

Syntax Description

This command has no arguments or keywords.

Command Default

No ND inspection policies are configured.

Command Modes

ND inspection policy configuration (config-nd-inspection)
RA guard policy configuration (config-ra-guard)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

The **drop-unsecure** command drops messages with no or invalid Cryptographically Generated Address (CGA) options or Rivest, Shamir, and Adelman (RSA) signature as per RFC 3971, *Secure Discovery (SeND)*. However, note that messages with an RSA signature or CGA options that do not conform with or are not verified per RFC 3972, *Cryptographically Generated Addresses (CGA)*, are dropped.

Use the **drop-unsecure** command after enabling ND inspection policy configuration mode using the **ipv6 nd inspection policy** command.

Examples

The following example defines an ND policy name as policy1, places the router in ND inspection policy configuration mode, and enables the router to drop messages with invalid CGA options or an invalid RSA signature:

```
Router(config)# ipv6 nd-inspection policy policy1
Router(config-nd-inspection)# drop-unsecure
```

Related Commands

Command	Description
ipv6 nd inspection policy	Defines the ND inspection policy name and enters ND inspection policy configuration mode.
ipv6 nd raguard policy	Defines the RA guard policy name and enter RA guard policy configuration mode.

dspfarm profile

To enter DSP farm profile configuration mode and define a profile for digital signal processor (DSP) farm services, use the **dspfarm profile** command in global configuration mode. To delete a disabled profile, use the **no** form of this command.

Cisco Unified Border Element

dspfarm profile *profile-identifier* {**conference** | **mtp** | **transcode**} [**security**]

no dspfarm profile *profile-identifier*

Cisco Unified Border Element (Enterprise) Cisco ASR 1000 Series Router

dspfarm profile *profile-identifier* {**transcode**}

no dspfarm profile *profile-identifier*

Cisco Integrated Services Routers Generation 2 (Cisco ISR G2)

dspfarm profile *profile-identifier* {**conference** [**video** [**homogeneous** | **heterogeneous** | **guaranteed-audio**]] | **mtp** | **transcode** [**video** | **universal**] } [**security**]

no dspfarm profile *profile-identifier*

Syntax Description

profile-identifier	Number that uniquely identifies a profile. Range is 1 to 65535. There is no default.
conference	Enables a profile for conferencing.
mtp	Enables a profile for Media Termination Point (MTP).
transcode	Enables a profile for transcoding.
security	Enables a profile for secure DSP farm services.
video	(Optional) Enables a profile for video conferencing or transcoding.
homogeneous	(Optional) Specifies that all video participants use the one video format that is configured in this profile. DSP resources are reserved to support the conference at configuration time. **Note** The homogeneous profiles only support one video codec.
heterogeneous	(Optional) Specifies that video participants can use the different video formats that are configured in the profile. You can configure up to 10 video codecs in the heterogeneous profile. DSP resources are reserved to support the different configurations at configuration time.
guaranteed-audio	(Optional) Specifies that video participants in a heterogeneous conference will at least have an audio connection. You can configure up to 10 video codecs in the guaranteed-audio profile. The DSP resources for audio streams are reserved at configuration time, but DSP resources to support video conferences are not reserved. If the video endpoint supports the video format specified in the profile and DSP resources are available when the participant joins the conference, the participant joins as a video conferee in the video conference.

Command Default If this command is not entered, no profiles are defined for the DSP farm services.

Command Modes Global configuration (config)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4(11)XW	The **security** keyword was added.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.4(22)T	Support for IPv6 was added.
15.0(1)M2 15.1(1)T	Support was modified for the Cisco IAD 2430, IAD 2431, IAD 2432, and IAD 2435, and the Cisco VG 202, VG 204, and VG 224 platforms.
Cisco IOS XE Release 3.2S	This command was modified. Support was added to the Cisco ASR 1000 Series Router. The **conference**, **mtp** and **security** keywords are not supported on the Cisco ASR 1000 Series Router in this release.
15.1(4)M	This command was modified. The **video** keyword was added.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines Use this command to create a new profile or delete a disabled profile. After you create a new profile in dspfarm profile configuration mode, use the **no shutdown** command to enable the profile configuration, allocate resources and associate the profile with the application(s). If the profile cannot be enabled due to lack of resources, the system prompts you with a message "Can not enable the profile due to insufficient resources, resources available to support X sessions; please modify the configuration and retry."

If the DSP farm profile is successfully created, you enter the DSP farm profile configuration mode. You can configure multiple profiles for the same service.

Use the **no dspfarm profile** command to delete a profile from the system. If the profile is active, you cannot delete it; you must first disable it using the **shutdown** command. To modify a DSP farm profile, use the **shutdown** command in dspfarm profile configuration mode before you begin configuration.

The *profile identifier* uniquely identifies a profile. If the service type and *profile identifier* are not unique, the user is prompted with a message to choose a different profile identifier.

You must use the **security** keyword in order to enable secure DSP farm services such as secure transcoding.

Effective with Cisco IOS Releases 15.0(1)M2 and 15.1(1)T, platform support for the Cisco IAD 2430, IAD 2431, IAD 2432, and IAD 2435, and the Cisco VG 202, VG 204, and VG 225 is modified. These platforms are designed as TDM-IP devices and are not expandable to install extra DSP resources. So even though the **conference** keyword appears in the command syntax, this DSP service is not configurable on these platforms. If you try to configure conferencing on these platforms, the command-line interface displays the following message: "`%This platform does not support Conferencing feature.`"

The **transcode** keyword also appears in the command syntax, but this DSP service is not available on the Cisco VG 202, VG 204, and VG 224 platforms. If you try to configure transcoding on these platforms, the CLI displays the following message: "`%This platform does not support Transcoding feature.`"

Cisco ASR 1000 Series Router

The support for dspfarm profile command was added on Cisco ASR 1000 Series Router from Cisco IOS XE Release 3.2 and later releases. The command is used to create a dspfarm profile for different services.

Note The secure DSP farm services is always enabled for SPA-DSP on Cisco ASR 1000 Series Router. Only **transcode** keyword is supported on Cisco ASR 1000 Series Router for Cisco IOS XE Release 3.2s. The **conference**, **media**, and **security** keywords are not supported on Cisco ASR 1000 Series Router for Cisco IOS XE Release 3.2s.

In order to configure a video dspfarm profile, you must set **voice-service dsp-reservation** command to be less than 100 percent.

To enable dspfarm profiles for voice services, you must use the **dsp services dspfarm** command under the voice-card submode.

Examples

The following example enables DSP farm services profile 20 for conferencing:

```
Router(config)# dspfarm profile 20 conference
```

Note the response if the profile is already being used:

```
Router(config)# dspfarm profile 6 conference

Profile id 6 is being used for service TRANSCODING
 please select a different profile id
```

The following example enables DSP farm services profile 1 for transcoding:

```
Router(config)# dspfarm profile 1 transcode
```

Video Conferences

The following example enables DSP farm services profile 99 for homogeneous video. The conference supports four participants under one format (Video codec H.263, qcif resolution, and a frame-rate of 15 f/s).

```
Router(config)# dspfarm profile 99 conference video homogeneous
Router(config-dspfarm-profile)# codec h263 qcif frame-rate 15
Router(config-dspfarm-profile)# maximum conference-participant 4
```

Related Commands

Command	Description
dsp service dspfarm	Configures the DSP farm services for a specified voice card.
shutdown (DSP farm profile)	Disables the DSP farm profile.
voice-card	Enters voice card configuration mode
voice-service dsp-reservation	Configures the percentage of DSP resources are reserved for voice services and enables video services to use the remaining DSP resources.

eigrp event-log-size

To set the size of the Enhanced Interior Gateway Routing Protocol (EIGRP) event log, use the **eigrp event-log-size** command in router configuration mode or address-family topology configuration mode. To reset the size of the EIGRP event log to its default value, use the **no** form of this command.

eigrp event-log-size *size*

no eigrp event-log-size

Syntax Description

size	Size of the EIGRP event log; valid values are from 0 to half of the available memory on the system at the time of configuration. Default value is 500.

Command Default

The EIGRP event log size is 500.

Command Modes

Router configuration (config-router)
Address-family topology configuration (config-router-af-topology)

Command History

Release	Modification
12.2(18)SXF	This command was introduced in Cisco IOS Release 12.2(18)SXF.
15.0(1)M	This command was modified. Address-family topology configuration mode was added.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

When the configured size (number of lines) of the event log is exceeded, the last configured number of lines is retained, and the log becomes a rolling number of events with the most recent at the top of the log.

Examples

The following example shows how to set the size of the EIGRP event log to 5000010:

```
Router# configure terminal
Router(config)# router eigrp 2
Router (config-router)# eigrp event-log-size 5000010
Router (config-router)#
```

The following example shows how to set the size of the EIGRP event log in an EIGRP named configuration to 10000:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 1
Router(config-router-af)# topology base
Router(config-router-af-topology)# eigrp event-log-size 10000
```

Related Commands

Command	Description
clear ip eigrp event	Clears the IP EIGRP event log.

eigrp log-neighbor-changes

To enable the logging of changes in Enhanced Interior Gateway Routing Protocol (EIGRP) neighbor adjacencies, use the **eigrp log-neighbor-changes** command in router configuration mode, address-family configuration mode, or service-family configuration mode. To disable the logging of changes in EIGRP neighbor adjacencies, use the **no** form of this command.

eigrp log-neighbor-changes

no eigrp log-neighbor-changes

Syntax Description

This command has no arguments or keywords.

Command Default

Adjacency changes are logged.

Command Modes

Router configuration (config-router)
Address-family configuration (config-router-af)
Service-family configuration (config-router-sf)

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.
15.0(1)M	This command was modified. Address-family configuration mode and service-family configuration mode were added.
12.2(33)SRE	This command was modified. Address-family configuration mode and service-family configuration mode were added.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

This command enables the logging of neighbor adjacency changes to monitor the stability of the routing system and to help detect problems. Logging is enabled by default. To disable the logging of neighbor adjacency changes, use the **no** form of this command.

To enable the logging of changes for EIGRP address-family neighbor adjacencies, use the **eigrp log-neighbor-changes** command in address-family configuration mode.

To enable the logging of changes for EIGRP service-family neighbor adjacencies, use the **eigrp log-neighbor-changes** command in service-family configuration mode.

Examples

The following configuration disables logging of neighbor changes for EIGRP process 209:

```
Router(config)# router eigrp 209
Router(config-router)# no eigrp log-neighbor-changes
```

The following configuration enables logging of neighbor changes for EIGRP process 209:

```
Router(config)# router eigrp 209
Router(config-router)# eigrp log-neighbor-changes
```

The following example shows how to disable logging of neighbor changes for EIGRP address-family with autonomous-system 4453:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# no eigrp log-neighbor-changes
Router(config-router-af)# exit-address-family
```

The following configuration enables logging of neighbor changes for EIGRP service-family process 209:

```
Router(config)# router eigrp 209
Router(config-router)# service-family ipv4 autonomous-system 4453
Router(config-router-sf)# eigrp log-neighbor-changes
Router(config-router-sf)# exit-service-family
```

Related Commands

Command	Description
address-family (EIGRP)	Enters address-family configuration mode to configure an EIGRP routing instance.
exit-address-family	Exits address-family configuration mode.
exit-service-family	Exits service-family configuration mode.
router eigrp	Configures the EIGRP routing process.
service-family	Specifies service-family configuration mode.

eigrp log-neighbor-warnings

To enable the logging of Enhanced Interior Gateway Routing Protocol (EIGRP) neighbor warning messages, use the **eigrp log-neighbor-warnings** command in router configuration mode, address-family configuration mode, or service-family configuration mode. To disable the logging of EIGRP neighbor warning messages, use the **no** form of this command.

eigrp log-neighbor-warnings [*seconds*]

no eigrp log-neighbor-warnings

Syntax Description

seconds	(Optional) The time interval (in seconds) between repeated neighbor warning messages. The range is from 1 to 65535. The default is 10.

Command Default

Neighbor warning messages are logged at 10-second intervals.

Command Modes

Router configuration (config-router)
Address-family configuration (config-router-af)
Service-family configuration (config-router-sf)

Command History

Release	Modification
12.0(5)	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. Address-family and service-family configuration modes were added.
12.2(33)SRE	This command was modified. Address-family and service-family configuration modes were added.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

When neighbor warning messages occur, they are logged by default. With this command, you can disable and enable neighbor warning messages, and you can configure the interval between repeated neighbor warning messages.

To enable the logging of warning messages for an EIGRP address family, use the **eigrp log-neighbor-warnings** command in address-family configuration mode.

To enable the logging of warning messages for an EIGRP service family, use the **eigrp log-neighbor-warnings** command in service-family configuration mode.

Examples

The following command will log neighbor warning messages for EIGRP process 209 and repeat the warning messages in 5-minute (300 seconds) intervals:

```
Router(config)# router eigrp 209
Router(config-router)# eigrp log-neighbor-warnings 300
```

The following example logs neighbor warning messages for the service family with autonomous system number 4453 and repeats the warning messages in five-minute (300 second) intervals:

```
Router(config)# router eigrp virtual-name
Router(config-router)# service-family ipv4 autonomous-system 4453
Router(config-router-sf)# eigrp log-neighbor-warnings 300
```

The following example logs neighbor warning messages for the address family with autonomous system number 4453 and repeats the warning messages in five-minute (300 second) intervals:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# eigrp log-neighbor-warnings 300
```

Related Commands

Command	Description
address-family (EIGRP)	Enters address-family configuration mode to configure an EIGRP routing instance.
exit-address-family	Exits address-family configuration mode.
exit-service-family	Exits service-family configuration mode.
router eigrp	Configures the EIGRP routing process.
service-family	Specifies service-family configuration mode.

eigrp router-id

To set the router ID used by Enhanced Interior Gateway Routing Protocol (EIGRP) when communicating with its neighbors, use the **eigrp router-id** command in router configuration mode, address-family configuration mode, or service-family configuration mode. To remove the configured router ID, use the **no** form of this command.

eigrp router-id *router-id*

no eigrp router-id [*router-id*]

Syntax Description

router-id	EIGRP router ID in IP address format.

Command Default

EIGRP automatically selects an IP address to use as the router ID when an EIGRP process is started. The highest local IP address is selected and loopback interfaces are preferred. The router ID is not changed unless the EIGRP process is removed with the **no router eigrp** command or if the router ID is manually configured with the **eigrp router-id** command.

Command Modes

Router configuration (config-router)
Address-family configuration (config-router-af)
Service-family configuration (config-router-sf)

Command History

Release	Modification
12.1	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. Address-family configuration mode and service-family configuration mode were added.
12.2(33)SRE	This command was modified. Address-family configuration mode and service-family configuration mode were added.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

The router ID is used to identify the originating router for external routes. If an external route is received with the local router ID, the route is discarded. The router ID can be configured with any IP address with two exceptions; 0.0.0.0 and 255.255.255.255 are not legal values and cannot be entered. A unique value should be configured for each router.

In EIGRP named IPv4, named IPv6, and Cisco Service Advertisement Framework (SAF) configurations, the *router-id* is also included for identifying internal routes and loop detection.

Examples

The following example configures 172.16.1.3 as a fixed router ID:

```
Router(config)# router eigrp 209
Router(config-router)# eigrp router-id 172.16.1.3
```

The following example configures 172.16.1.3 as a fixed router ID for service-family autonomous-system 4533:

```
Router(config)# router eigrp 209
Router(config-router)# service-family ipv4 autonomous-system 4453
Router(config-router-sf)# eigrp router-id 172.16.1.3
```

The following example configures 172.16.1.3 as a fixed router ID for address-family autonomous-system 4533:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# eigrp router-id 172.16.1.3
```

Related Commands

Command	Description
address-family (EIGRP)	Enters address-family configuration mode to configure an EIGRP routing instance.
router eigrp	Configures the EIGRP routing process.
service-family	Specifies service-family configuration mode.

eigrp stub

To configure a router as a stub using Enhanced Interior Gateway Routing Protocol (EIGRP), use the **eigrp stub** command in router configuration mode or address-family configuration mode. To disable the EIGRP stub routing feature, use the **no** form of this command.

eigrp stub [**receive-only**] [**leak-map** *name*] [**connected**] [**static**] [**summary**] [**redistributed**]

no eigrp stub

Syntax Description

receive-only	(Optional) Sets the router as a receive-only neighbor.
leak-map *name*	(Optional) Allows dynamic prefixes based on a leak map.
connected	(Optional) Advertises connected routes.
static	(Optional) Advertises static routes.
summary	(Optional) Advertises summary routes.
redistributed	(Optional) Advertises redistributed routes from other protocols and autonomous systems.

Command Default

Stub routing is not enabled by default.

Command Modes

Router configuration (config-router)
Address-family configuration (config-router-af)

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.0(15)S	This command was integrated into Cisco IOS Release 12.0(15)S.
12.2	The **redistributed** 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.
15.0(1)M	This command was modified. Address-family configuration mode was added to support EIGRP named configurations. The **leak-map** keyword and *name* argument were added. This command replaces the **stub** command.
12.2(33)SRE	This command was modified. Address-family configuration mode was added to support EIGRP named configurations. The **leak-map** keyword and *name* argument were added. This command replaces the **stub** command.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.

Release	Modification
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
12.2(33)SXI4	This command was modified. Address-family configuration mode was added to support EIGRP named configurations. The **leak-map** keyword and *name* argument were added. This command replaces the **stub** command.

Usage Guidelines

Use the **eigrp stub** command to configure a router as a stub where the router directs all IP traffic to a distribution router, unless stub leaking is configured.

The **eigrp stub** command can be modified with several options, and these options can be used in any combination except for the **receive-only** keyword. The **receive-only** keyword will restrict the router from sharing any of its routes with any other router in that EIGRP autonomous system, and the **receive-only** keyword will not permit any other option to be specified because it prevents any type of route from being sent. The four other optional keywords (**connected**, **static**, **summary**, **leak-map**, and **redistributed**) can be used in any combination but cannot be used with the **receive-only** keyword.

If any of these five keywords is used with the **eigrp stub** command, only the route types specified by the particular keyword(s) will be sent. Route types specified by the remaining keywords will not be sent.

The **connected** keyword permits the EIGRP stub routing feature to send connected routes. If the connected routes are not covered by a network statement, it may be necessary to redistribute connected routes with the **redistribute connected** command under the EIGRP process. This option is enabled by default.

The **static** keyword permits the EIGRP stub routing feature to send static routes. Without the configuration of this option, EIGRP will not send any static routes, including internal static routes that normally would be automatically redistributed. It will still be necessary to redistribute static routes with the **redistribute static** command.

The **summary** keyword permits the EIGRP stub routing feature to send summary routes. Summary routes can be created manually with the **summary address** command or automatically at a major network border router with the **auto-summary** command enabled. This option is enabled by default.

The **redistributed** keyword permits the EIGRP stub routing feature to send other routing protocols and autonomous systems. Without the configuration of this option, EIGRP will not advertise redistributed routes.

The **leak-map** keyword permits the EIGRP stub routing feature to reference a leak map that identifies routes that are allowed to be advertised on an EIGRP stub router that would normally have been suppressed.

Examples

In the following example, the **eigrp stub** command is used to configure the router as a stub that advertises connected and summary routes:

```
Router(config)# router eigrp 1
Router(config-router)# network 10.0.0.0
Router(config-router)# eigrp stub
```

In the following named configuration example, the **eigrp stub** command is used to configure the router as a stub that advertises routes learned from a directly connected client:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# network 10.0.0.0
Router(config-router-af)# eigrp stub connected
```

In the following example, the **eigrp stub** command is issued with the **connected** and **static** keywords to configure the router as a stub that advertises connected and static routes (sending summary routes will not be permitted):

```
Router(config)# router eigrp 1
Router(config-router)# network 10.0.0.0
Router(config-router)# eigrp stub connected static
```

In the following named configuration example, the **eigrp stub** command is issued with the **connected** and **static** keywords to configure the router as a stub that advertises connected and static routes (sending summary routes will not be permitted):

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# network 10.0.0.0
Router(config-router-af)# eigrp stub connected static
```

In the following example, the **eigrp stub** command is issued with the **receive-only** keyword to configure the router as a receive-only neighbor (connected, summary, and static routes will not be sent):

```
Router(config)# router eigrp 1
Router(config-router)# network 10.0.0.0 eigrp
Router(config-router)# eigrp stub receive-only
```

In the following named configuration example, the **eigrp stub** command is issued with the **receive-only** keyword to configure the router as a receive-only neighbor (connected, summary, and static routes will not be sent):

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# network 10.0.0.0
Router(config-router-af)# eigrp stub receive-only
```

In the following example, the **eigrp stub** command is issued with the **redistributed** keyword to configure the router to advertise other protocols and autonomous systems:

```
Router(config)# router eigrp 1
Router(config-router)# network 10.0.0.0 eigrp
Router(config-router)# eigrp stub redistributed
```

In the following named configuration example, the **eigrp stub** command is issued with the **redistributed** keyword to configure the router to advertise other protocols and autonomous systems:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# network 10.0.0.0
Router(config-router-af) eigrp stub redistributed
```

In the following example, the **eigrp stub** command is issued with the **leak-map** *name* keyword/argument pair to configure the router to reference a leak map that identifies routes that would normally have been suppressed:

```
Router(config)# router eigrp
Router(config-router)# network 10.0.0.0
Router(config-router) eigrp stub leak-map map1
```

In the following named configuration example, the **eigrp stub** command is issued with the **leak-map** *name* keyword/argument pair to configure the router to reference a leak map that identifies routes that would normally have been suppressed:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
```

```
Router(config-router-af)# network 10.0.0.0
Router(config-router-af) eigrp stub leak-map map1
```

Related Commands

Command	Description
address-family (EIGRP)	Enters address-family configuration mode to configure an EIGRP routing instance.
network (EIGRP)	Specifies the network for an EIGRP routing process.
router eigrp	Configures the EIGRP address-family process.

encapsulation

To set the encapsulation method used by the interface, use the **encapsulation** command in interface configuration mode. To remove the encapsulation, use the **no** form of this command.

encapsulation *encapsulation-type*

no encapsulation *encapsulation-type*

Syntax Description

encapsulation-type	Encapsulation type; one of the following keywords: • **atm-dxi**—ATM Mode-Data Exchange Interface. • **bstun**—Block Serial Tunnel. • **dot1q** *vlan-id* [**native**]—Enables IEEE 802.1q encapsulation of traffic on a specified subinterface in VLANs. The *vlan-id* argument is a virtual LAN identifier. The valid range is from 1 to 1000. The optional **native** keyword sets the PVID value of the port to the *vlan-id* value. • **frame-relay**—Frame Relay (for serial interface). • **hdlc**—High-Level Data Link Control (HDLC) protocol for serial interface. This encapsulation method provides the synchronous framing and error detection functions of HDLC without windowing or retransmission. This is the default for synchronous serial interfaces. • **isl** *vlan-id*—Inter-Switch Link (ISL) (for VLANs). • **lapb**—X.25 Link Access Procedure, Balanced. Data link layer protocol (LAPB) DTE operation (for serial interface). • **ppp**—PPP (for serial interface). • **sde** *said*—IEEE 802.10. The *said* argument is a security association identifier. This value is used as the VLAN identifier. The valid range is from 0 to 0xFFFFFFFE. • **sdlc**—IBM serial Systems Network Architecture (SNA). • **sdlc-primary**—IBM serial SNA (for primary serial interface). • **sdlc-secondary**—IBM serial SNA (for secondary serial interface). • **slip**—Specifies Serial Line Internet Protocol (SLIP) encapsulation for an interface configured for dedicated asynchronous mode or dial-on-demand routing (DDR). This is the default for asynchronous interfaces. • **smds**—Switched Multimegabit Data Services (SMDS) (for serial interface). • **ss7**—Sets the encapsulation type to SS7 and overrides the serial interface objects high-level data link control (HDLC) default.

Defaults

The default depends on the type of interface. For example, synchronous serial interfaces default to HDLC and asynchronous interfaces default to SLIP.

Command Modes Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
10.3	The **sde** keyword was added to support IEEE 802.10
11.1	The **isl** keyword was added to support the Interswitch Link (ISL) Cisco protocol for interconnecting multiple switches and routers, and for defining virtual LAN (VLAN) topologies.
11.3(4)T	The **tr-isl trbrf-vla**n keyword was added to support TRISL, a Cisco proprietary protocol for interconnecting multiple routers and switches and maintaining VLAN information as traffic goes between switches.
12.0(1)T	The **dot1q** keyword was added to support IEEE 8021q standard for encapsulation of traffic on a specified subinterface in VLANs.
12.1(3)T	The **native** keyword was added.
12.2(11)T	This command was modified to include the **ss7** keyword in support of integrated signaling link terminal capabilities.
12.2(13)T	Support for IPv6 was added.
12.3(2)T	The **tr-isl trbrf-vla**n keyword was removed because support for the TRISL 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.
Cisco IOS XE Release 2.5	This command was updated. It was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

SLIP and PPP

To use SLIP or PPP, the router or access server must be configured with an IP routing protocol or with the **ip host-routing** command. This configuration is done automatically if you are using old-style **slip address** commands. However, you must configure it manually if you configure SLIP or PPP via the **interface async** command.

On lines configured for interactive use, encapsulation is selected by the user when they establish a connection with the **slip** or **ppp** EXEC command.

IP Control Protocol (IPCP) is the part of PPP that brings up and configures IP links. After devices at both ends of a connection communicate and bring up PPP, they bring up the control protocol for each network protocol that they intend to run over the PPP link such as IP or IPX. If you have problems passing IP packets and the **show interface** command shows that line is up, use the **negotiations** command to see if and where the negotiations are failing. You might have different versions of software running, or different versions of PPP, in which case you might need to upgrade your software or turn off PPP option negotiations. All IPCP options as listed in RFC 1332, *PPP Internet Protocol Control Protocol (IPCP)*, are supported on asynchronous lines. Only Option 2, TCP/IP header compression, is supported on synchronous interfaces.

PPP echo requests are used as keepalive packets to detect line failure. The **no keepalive** command can be used to disable echo requests. For more information about the **no keepalive** command, refer to the chapter "IP Services Commands" in the *Cisco IOS IP Command Reference, Volume 1 of 4: Addressing and Services* and to the chapter "Configuring IP Services" in the *Cisco IOS IP Configuration Guide*.

To use SLIP or PPP, the Cisco IOS software must be configured with an IP routing protocol or with the **ip host-routing** command. This configuration is done automatically if you are using old-style **slip address** commands. However, you must configure it manually if you configure SLIP or PPP via the **interface async** command.

Note Disable software flow control on SLIP and PPP lines before using the **encapsulation** command.

SS7

The SS7 encapsulation command is new with the Integrated SLT feature and is available only for interface serial objects created by the **channel-group** command. For network access server (NAS) platforms, the encapsulation for channel group serial interface objects defaults to HDLC. You must explicitly set the encapsulation type to SS7 to override this default.

When encapsulation is set to SS7, the encapsulation command for that object is no longer available. A serial SS7 link is deleted only when its associated dial feature card (DFC) card is removed. As with existing Cisco 26*x*x-based SLTs, you do not need to specify whether the SS7 link is to be used as an A-link or an F-link.

By itself this command does not select the correct encapsulation type. Therefore, once created, you must set the encapsulation type to the new SS7 value, as well as assign a session channel ID to the link at the serial interface command level. The configuration on a digital SS7 link can be saved **(no shutdow**n) only when its encapsulation is successfully set to SS7 and it has been assigned a channel identifier.

VLANs

Do not configure encapsulation on the native VLAN of an IEEE 802.1q trunk without the **native** keyword. (Always use the **native** keyword when the *vlan-id* is the ID of the IEEE 802.1q native VLAN.)

For detailed information on use of this command with VLANs, refer to the *Cisco IOS Switching Services Configuration Guide* and the *Cisco IOS Switching Services Command Reference*.

Examples

The following example shows how to reset HDLC serial encapsulation on serial interface 1:

```
Router(config)# interface serial 1
Router(config-if)# encapsulation hdlc
```

The following example shows how to enable PPP encapsulation on serial interface 0:

```
Router(config)# interface serial 0
Router(config-if)# encapsulation ppp
```

The following example shows how to configure async interface 1 for PPP encapsulation:

```
Router(config)# interface async 1
Router(config-if)# encapsulation ppp
```

To learn more about the virtual serial interface and check SS7 encapsulation, enter the **show interfaces serial** *slot*/*trunk*:*channel-group* command in privileged EXEC mode, as in the following example:

```
Router# show interfaces serial 7/3:1

Serial7/3:1 is up, line protocol is down
 Hardware is PowerQUICC Serial
 MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
  reliability 255/255, txload 4/255, rxload 1/255
 Encapsulation SS7 MTP2, loopback not set
 Keepalive set (10 sec)
 Last input never, output 00:00:00, output hang never
 Last clearing of "show interface" counters 03:53:40
 Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 26000 bits/sec, 836 packets/sec
  0 packets input, 0 bytes, 0 no buffer
  Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  11580159 packets output, 46320636 bytes, 0 underruns
  0 output errors, 0 collisions, 1 interface resets
  0 output buffer failures, 0 output buffers swapped out
  2 carrier transitions
  DCD=up DSR=down DTR=down RTS=down CTS=down
```

Related Commands

Command	Description
channel-group	Assigns a channel group and selects the DSO time slots desired for SS7 links.
encapsulation x25	Specifies operation of a serial interface as an X.25 device.
keepalive	Sets the keepalive timer for a specific interface.
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.
ppp bap call	Sets PPP BACP call parameters.
slip	Starts a serial connection to a remote host using SLIP.

encapsulation frame-relay mfr

To create a multilink Frame Relay bundle link and to associate the link with a bundle, use the **encapsulation frame-relay mfr** command in interface configuration mode. To remove the bundle link from the bundle, use the **no** form of this command.

encapsulation frame-relay mfr *number* [*name*]

no encapsulation frame-relay mfr *number* [*name*]

Syntax Description

number	Interface number of the multilink Frame Relay bundle with which this bundle link will be associated.
name	(Optional) Bundle link identification (LID) name. The name can be up to 49 characters long. The default is the name of the physical interface.

Command Default

Frame Relay encapsulation is not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(17)S	This command was introduced on the Cisco 12000 series routers.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(24)S	This command was implemented on VIP-enabled Cisco 7500 series routers.
12.3(4)T	Support for this command on VIP-enabled Cisco 7500 series routers was integrated into Cisco IOS Release 12.3(4)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.
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.
12.0(33)S	Support for IPv6 was added. This command was implemented on the Cisco 12000 series routers.

Usage Guidelines

Use the *name* argument to assign a LID name to a bundle link. This name will be used to identify the bundle link to peer devices and to enable the devices to determine which bundle links are associated with which bundles. The LID name can also be assigned or changed by using the **frame-relay multilink lid** command on the bundle link interface. If the LID name is not assigned, the default name is the name of the physical interface.

Tips To minimize latency that results from the arrival order of packets, we recommend bundling physical links of the same line speed in one bundle.

To remove a bundle link from a bundle, use the **no encapsulation frame-relay mfr** command or configure a new type of encapsulation on the interface by using the **encapsulation** command.

Examples

The following example shows serial interface 0 being associated as a bundle link with bundle interface "mfr0." The bundle link identification name is "BL1."

```
interface mfr0
!
interface serial 0
 encapsulation frame-relay mfr0 BL1
```

Related Commands

Command	Description
debug frame-relay multilink	Displays debug messages for multilink Frame Relay bundles and bundle links.
encapsulation	Sets the encapsulation method used by the interface.
frame-relay multilink lid	Assigns a LID name to a multilink Frame Relay bundle link.
show frame-relay multilink	Displays configuration information and statistics about multilink Frame Relay bundles and bundle links.

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.

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-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 27.
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 27 lists the available enrollment methods.

Table 27 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.

eui-interface

To use the Media Access Control (MAC) address from a specified interface for deriving the IPv6 mobile home address, use the **eui-interface** command in IPv6 mobile router configuration mode. To disable this function, use the **no** form of this command.

eui-interface *interface-type interface-number*

no eui-interface *interface-type interface-number*

Syntax Description

interface-type interface-number	Interface type and number from which the MAC address is derived.

Command Default

A MAC address is not used to derive the IPv6 mobile home address.

Command Modes

IPv6 mobile router configuration (IPv6-mobile-router)

Command History

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

Usage Guidelines

Use the **eui-interface** command to physically connect to the MAC to get the EUI-64 interface ID.

Examples

In the following example, the router derives the EUI-64 interface ID from the specified interface:

```
eui-interface Ethernet 0/0
```

Related Commands

Command	Description
ipv6 mobile router	Enables IPv6 NEMO functionality on the router and places the router in IPv6 mobile router mode.

evaluate (IPv6)

To nest an IPv6 reflexive access list within an IPv6 access list, use the **evaluate** (IPv6) command in IPv6 access list configuration mode. To remove the nested IPv6 reflexive access list from the IPv6 access list, use the **no** form of this command.

evaluate *access-list-name* [**sequence** *value*]

no evaluate *access-list-name* [**sequence** *value*]

Syntax Description

access-list-name	The name of the IPv6 reflexive access list that you want evaluated for IPv6 traffic entering your internal network. This is the name defined in the **permit** (IPv6) command. Names cannot contain a space or quotation mark, or begin with a numeric.
sequence *value*	(Optional) Specifies the sequence number for the IPv6 reflexive access list. The acceptable range is from 1 to 4294967295.

Command Default

IPv6 reflexive access lists are not evaluated.

Command Modes

IPv6 access list configuration

Command History

Release	Modification
12.0(23)S	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(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.

Usage Guidelines

The **evaluate** (IPv6) command is similar to the **evaluate** (IPv4) command, except that it is IPv6-specific.

This command is used to achieve IPv6 reflexive filtering, a form of session filtering.

Before this command will work, you must define the IPv6 reflexive access list using the **permit** (IPv6) command.

This command nests an IPv6 reflexive access list within an IPv6 access control list (ACL).

If you are configuring an IPv6 reflexive access list for an external interface, the IPv6 ACL should be one that is applied to inbound traffic. If you are configuring IPv6 reflexive access lists for an internal interface, the IPv6 ACL should be one that is applied to outbound traffic. (In other words, use the access list opposite of the one used to define the IPv6 reflexive access list.)

This command allows IPv6 traffic entering your internal network to be evaluated against the reflexive access list. Use this command as an entry (condition statement) in the IPv6 ACL; the entry “points” to the IPv6 reflexive access list to be evaluated.

As with all IPv6 ACL entries, the order of entries is important. Normally, when a packet is evaluated against entries in an IPv6 ACL, the entries are evaluated in sequential order, and when a match occurs, no more entries are evaluated. With an IPv6 reflexive access list nested in an IPv6 ACL, the IPv6 ACL entries are evaluated sequentially up to the nested entry, then the IPv6 reflexive access list entries are evaluated sequentially, and then the remaining entries in the IPv6 ACL are evaluated sequentially. As usual, after a packet matches any of these entries, no more entries will be evaluated.

Note IPv6 reflexive access lists do not have any implicit deny or implicit permit statements.

Examples

The **evaluate** command in the following example nests the temporary IPv6 reflexive access lists named TCPTRAFFIC and UDPTRAFFIC in the IPv6 ACL named OUTBOUND. The two reflexive access lists are created dynamically (session filtering is "triggered") when incoming TCP or UDP traffic matches the applicable permit entry in the IPv6 ACL named INBOUND. The OUTBOUND IPv6 ACL uses the temporary TCPTRAFFIC or UDPTRAFFIC access list to match (evaluate) outgoing TCP or UDP traffic related to the triggered session. The TCPTRAFFIC and UDPTRAFFIC lists time out automatically when no IPv6 packets match the permit statement that triggered the session (the creation of the temporary reflexive access list).

Note The order of IPv6 reflexive access list entries is not important because only permit statements are allowed in IPv6 reflexive access lists and reflexive access lists do not have any implicit conditions. The OUTBOUND IPv6 ACL simply evaluates the UDPTRAFFIC reflexive access list first and, if there were no matches, the TCPTRAFFIC reflexive access list second. Refer to the **permit** command for more information on configuring IPv6 reflexive access lists.

```
ipv6 access-list INBOUND
  permit tcp any any eq bgp reflect TCPTRAFFIC
  permit tcp any any eq telnet reflect TCPTRAFFIC
  permit udp any any reflect UDPTRAFFIC

ipv6 access-list OUTBOUND
  evaluate UDPTRAFFIC
  evaluate TCPTRAFFIC
```

Related Commands

Command	Description
ipv6 access-list	Defines an IPv6 access list and enters IPv6 access list configuration mode.
permit (IPv6)	Sets permit conditions for an IPv6 access list.
show ipv6 access-list	Displays the contents of all current IPv6 access lists.

event-log

To enable event logging for applications, use the **event-log** command in application configuration monitor configuration mode. To disable event logging, use the **no** form of this command.

event-log [**size** [*number of events*]] [**one-shot**] [**pause**]

no event-log

Syntax Description

size [*number of events*]	(Optional) Maximum number of OSPF events in the event log.
one-shot	(Optional) Mode that enables the logging of new events at one specific point in time. The event logging mode is cyclical by default, meaning that all new events are logged as they occur.
pause	(Optional) Enables the user to pause the logging of any new events at any time, while keeping the current events in the log.

Command Default

By default, event logging is not enabled.
When event logging is enabled, it is cyclical by default.

Command Modes

Application configuration monitor configuration mode
OSPF for IPv6 router configuration mode

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application event-log** command.
12.2(33)SRC	Support for IPv6 was added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 series routers.
15.0(1)M	This command was integrated into Cisco IOS Release 12.5(1)M.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

This command enables event logging globally for all voice applications. To enable or disable event logging for a specific application, use one of the following commands:

param event-log (application parameter configuration mode)

paramspace appcommon event-log (service configuration mode)

Note To prevent event logging from adversely impacting system resources for production traffic, the gateway uses a throttling mechanism. When free processor memory drops below 20-percent, the gateway automatically disables all event logging. It resumes event logging when free memory rises above 30 percent. While throttling is occurring, the gateway does not capture any new event logs even if event logging is enabled. You should monitor free memory and enable event logging only when necessary for isolating faults.

Examples

The following example shows event logging enabled:

```
application
 monitor
  event-log
```

The following example shows OSPF for IPv6 event logging enabled. The router instance is 1, the event-log size is 10,000, and the mode is one-shot.

```
ipv6 router ospf 1
 event-log size 10000 one-shot
```

Related Commands

Command	Description
call application event-log	Enables event logging for all voice application instances.
event-log dump ftp	Enables the gateway to write the contents of the application event log buffer to an external file.
event-log error-only	Restricts event logging to error events only for application instances.
event-log max-buffer-size	Sets the maximum size of the event log buffer for each application instance.
param event-log	Enables or disables event logging for a package.
paramspace appcommon event-log	Enables or disables event logging for a service (application).

event-log (OSPFv3)

To enable Open Shortest Path First version 3 (OSPFv3) event logging in an IPv4 OSPFv3 process, use the **event-log** command in OSPFv3 router configuration mode. To disable this feature, use the **no** version of the command.

event-log [**one-shot** | **pause** | **size** *number-of-events*]

Syntax Description

one-shot	(Optional) Disables OSPFv3 event logging when the log buffer becomes full.
pause	(Optional) Pauses the event logging function.
size *number-of-events*	(Optional) Configures the maximum number of events stored in the event log. The range is from 1 through 65534.

Command Default

Event logging is not enabled.

Command Modes

OSPFv3 router configuration mode (config-router)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

Examples

The following examples show how to enable event logging in an IPv4 OSPFv3 process:

```
Router(config)# router ospfv3 1
Router(config-router)# event-log
```

Related Commands

Command	Description
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

explicit-prefix

To register IPv6 prefixes connected to the IPv6 mobile router, use the **explicit-prefix** command in IPv6 mobile router configuration mode. To disable this function, use the **no** form of this command.

explicit-prefix

no explicit-prefix

Syntax Description

This command has no arguments or keywords.

Command Default

No IPv6 prefixes are specified.

Command Modes

IPv6 mobile router configuration (IPv6-mobile-router)

Command History

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

Usage Guidelines

The mobile router presents a list of prefixes to the home agent as part of the binding update procedure. If the home agent determines that the mobile router is authorized to use these prefixes, it sends a bind acknowledgment message.

Examples

The following example shows how to register connected IPv6 prefixes:

```
Router(IPv6-mobile-router)# explicit-prefix
```

Related Commands

Command	Description
ipv6 mobile router	Enables IPv6 NEMO functionality on the router and places the router in IPv6 mobile router mode.

fabric switching-mode allow

To enable various switching modes in the presence of two or more fabric-enabled switching modules, use the **fabric switching-mode allow** command in global configuration mode. To disable the settings, use the **no** form of this command.

fabric switching-mode allow {**bus-mode** | **dcef-only** | **truncated** [**threshold** [*mod*]]}

no fabric switching-mode allow {**bus-mode** | **truncated** [**threshold**]}

Syntax Description

bus-mode	Specifies a module to run in bus mode.
dcef-only	Allows switching in distributed Cisco Express Forwarding (dCEF)-only mode.
truncated	Specifies a module to run in truncated mode.
threshold *mod*	(Optional) Specifies the number of fabric-enabled modules for truncated switching mode; see the "Usage Guidelines" section for additional information.

Command Default

The truncated mode is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)SX	This command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	This command was modified. This command supports the Supervisor Engine 2.
12.2(18)SXD1	This command was modified. The **dcef-only** keyword was added on the Supervisor Engine 2.
12.2(18)SXE	This command was modified. Support for OIR performance enhancement and the **dcef-only** keyword was added on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was modified. This command was introduced on the Supervisor Engine 720-10GE.

Usage Guidelines

This command is not supported on Catalyst 6500 or Cisco 7600 series routers that are configured with a Supervisor Engine 32.

Ethernet ports are not disabled when this command is entered on a Supervisor Engine 720-10GE. This command is also supported with Supervisor Engine 720 starting with Release 12.2(33)SXI2. However, prior to Release 12.2(33)SXI2, if all the installed switching modules have Distributed Forwarding Cards (DFCs), enter the **fabric switching-mode allow dcef-only** command to disable the Ethernet ports on both supervisor engines. Entering this command ensures that all modules are operating in dCEF-only mode and simplifies switchover to the redundant supervisor engine.

With a Supervisor Engine 2 and Release 12.2(18)SXD1 and later releases, if all the installed switching modules have DFCs, enter the **fabric switching-mode allow dcef-only** command to disable the Ethernet ports on the redundant supervisor engine. Entering this command ensures that all modules are operating in dCEF-only mode.

Note The **fabric switching-mode allow dcef-only** command is accepted only in stateful switchover (SSO) redundancy mode.

Bus mode—Supervisor engines use this mode for traffic between nonfabric-enabled modules and for traffic between a nonfabric-enabled module and a fabric-enabled module. In this mode, all traffic passes between the local bus and the supervisor engine bus.

dCEF-only—Supervisor engines, both active and redundant, operate as nonfabric-capable modules with their uplink ports relying on the Policy Feature Card (PFC) on the active supervisor engine for all forwarding decisions. For the Supervisor 720-10G, the uplink ports on both the active and standby routers will remain active. If all other modules are operating in dCEF-only mode, module Online Insertion and Removal (OIR) is nondisruptive.

Note The system message "PSTBY-2-CHUNKPARTIAL: Attempted to destroy partially full chunk, chunk 0xB263638, chunk name: MET FREE POOL" is displayed on the Supervisor Engine if both the **fabric switching-mode allow dcef-only** and **ipv6 mfib hardware-switching uplink** commands are configured. The router will ignore the command configured last.

Truncated mode—Supervisor engines use this mode for traffic between fabric-enabled modules when there are both fabric-enabled and nonfabric-enabled modules installed. In this mode, line cards send a truncated version of the traffic (the first 64 bytes of the frame) over the Catalyst bus.

Compact mode—Supervisor engines use this mode for all traffic when only fabric-enabled modules are installed. In this mode, a compact version of the Desktop Bus (DBus) header is forwarded over the Catalyst bus, which provides the best possible centralized forwarding performance.

A fabric-enabled module has an additional connection directly to the switch fabric. Fabric-enabled modules forward packets in compressed mode, where only the header is sent to the Supervisor Engine and the full packet is forwarded directly from one line card to another.

To prevent use of nonfabric-enabled modules or to prevent fabric-enabled modules from using bus mode, enter the **no fabric switching-mode allow bus-mode** command.

Caution Entering the **no fabric switching-mode allow bus-mode** command removes power from any nonfabric-enabled modules that are installed.

The **fabric switching-mode allow** command affects Supervisor engines that are configured with a minimum of two fabric-enabled modules.

You can enter the **fabric switching-mode allow truncated** command to unconditionally allow truncated mode.

You can enter the **no fabric switching-mode allow truncated** command to allow truncated mode if the threshold is met.

You can enter the **no fabric switching-mode allow bus-mode** command to prevent any module from running in bus mode.

To return to the default truncated-mode threshold, enter the **no fabric switching-mode allow truncated threshold** command.

The valid value for *mod* is the threshold value.

Examples

The following example shows how to specify truncated mode:

```
Router(config)# fabric switching-mode allow truncated
```

Related Commands

Command	Description
ipv6 mfib hardware-switching uplink	Configures MFIB hardware switching for IPv6 multicast packets on a global basis.
show fabric	Displays the information about the crossbar fabric.

fingerprint

To preenter a fingerprint that can be matched against the fingerprint of a certification authority (CA) certificate during authentication, use the **fingerprint** command in ca-trustpoint configuration mode. To remove the preentered fingerprint, use the **no** form of this command.

fingerprint *ca-fingerprint*

no fingerprint *ca-fingerprint*

Syntax Description

ca-fingerprint	Certificate fingerprint.

Defaults

A fingerprint is not preentered for a trustpoint, and if the authentication request is interactive, you must verify the fingerprint that is displayed during authentication of the CA certificate. If the authentication request is noninteractive, the certificate will be rejected without a preentered fingerprint.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.3(12)	This command was introduced. This release supports only message digest algorithm 5 (MD5) fingerprints.
12.3(13)T	Support was added for Secure Hash Algorithm 1 (SHA1), but only for Cisco IOS T releases.
12.4(24)T	Support for IPv6 Secure Neighbor Discovery (SeND) was added.

Usage Guidelines

Note An authentication request made using the CLI is considered an interactive request. An authentication request made using HTTP or another management tool is considered a noninteractive request.

Preenter the fingerprint if you want to avoid responding to the verify question during CA certificate authentication or if you will be requesting authentication noninteractively. The preentered fingerprint may be either the MD5 fingerprint or the SHA1 fingerprint of the CA certificate.

If you are authenticating a CA certificate and the fingerprint was preentered, if the fingerprint matches that of the certificate, the certificate is accepted. If the preentered fingerprint does not match, the certificate is rejected.

If you are requesting authentication noninteractively, the fingerprint must be preentered or the certificate will be rejected. The verify question will not be asked when authentication is requested noninteractively.

If you are requesting authentication interactively without preentering the fingerprint, the fingerprint of the certificate will be displayed, and you will be asked to verify it.

Examples

The following example shows how to preenter an MD5 fingerprint before authenticating a CA certificate:

```
Router(config)# crypto pki trustpoint myTrustpoint
Router(ca-trustpoint)# fingerprint 6513D537 7AEA61B7 29B7E8CD BBAA510B
Router(ca-trustpoint) exit
Router(config)# crypto pki authenticate myTrustpoint
Certificate has the following attributes:
       Fingerprint MD5: 6513D537 7AEA61B7 29B7E8CD BBAA510B
      Fingerprint SHA1: 998CCFAA 5816ECDE 38FC217F 04C11F1D DA06667E
Trustpoint Fingerprint: 6513D537 7AEA61B7 29B7E8CD BBAA510B
Certificate validated - fingerprints matched.
Trustpoint CA certificate accepted.
Router (config)#
```

The following is an example for Cisco Release 12.3(12). Note that the SHA1 fingerprint is not displayed because it is not supported by this release.

```
Router(config)# crypto ca trustpoint myTrustpoint
Router(ca-trustpoint)# fingerprint 6513D537 7AEA61B7 29B7E8CD BBAA510B
Router(ca-trustpoint)# exit
Router(config)# crypto ca authenticate myTrustpoint
Certificate has the following attributes:
           Fingerprint: 6513D537 7AEA61B7 29B7E8CD BBAA510B
Trustpoint Fingerprint: 6513D537 7AEA61B7 29B7E8CD BBAA510B
Certificate validated - fingerprints matched.
Trustpoint CA certificate accepted.
Router(config)#
```

Related Commands

Command	Description
crypto ca authenticate	Authenticates the CA (by getting the certificate of the CA).
crypto ca trustpoint	Declares the CA that your router should use.

frame-relay interface-dlci

To assign a data-link connection identifier (DLCI) to a specified Frame Relay subinterface on the router or access server, to assign a specific permanent virtual circuit (PVC) to a DLCI, or to apply a virtual template configuration for a PPP session, use the **frame-relay interface-dlci** command in interface configuration mode. To remove this assignment, use the **no** form of this command.

frame-relay interface-dlci *dlci* [**ietf** | **cisco**] [**voice-cir** *cir*] [**ppp** *virtual-template-name*]

no frame-relay interface-dlci *dlci* [**ietf** | **cisco**] [**voice-cir** *cir*] [**ppp** *virtual-template-name*]

BOOTP Server Only

frame-relay interface-dlci *dlci* [**protocol ip** *ip-address*]

no frame-relay interface-dlci *dlci* [**protocol ip** *ip-address*]

Syntax Description

dlci	DLCI number to be used on the specified subinterface.
ietf	(Optional) Specifies Internet Engineering Task Force (IETF) as the type of Frame Relay encapsulation.
cisco	(Optional) Specifies Cisco encapsulation as the type of Frame Relay encapsulation.
voice-cir *cir*	(Optional; supported on the Cisco MC3810 only.) Specifies the upper limit on the voice bandwidth that may be reserved for this DLCI. The default is the committed information rate (CIR) configured for the Frame Relay map class. For more information, see the "Usage Guidelines" section.
ppp	(Optional) Enables the circuit to use the PPP in Frame Relay encapsulation.
virtual-template-name	(Optional) Name of the virtual template interface to apply the PPP connection to.
protocol ip *ip-address*	(Optional) Indicates the IP address of the main interface of a new router or access server onto which a router configuration file is to be automatically installed over a Frame Relay network. Use this option only when this device will act as the BOOTP server for automatic installation over Frame Relay.

Command Default

No DLCI is assigned.

Command Modes

Interface configuration (config-if)
Subinterface configuration (config-subif)

Command History

Release	Modification
10.0	This command was introduced.
11.3(1)MA	The **voice-encap** option was added for the Cisco MC3810.
12.0(1)T	The **ppp** keyword and *virtual-template-name* argument were added.
12.0(2)T	The **voice-cir** option was added for the Cisco MC3810.
12.0(3)T	The **x25 profile** keyword was added.
12.0(4)T	Usage guidelines for the Cisco MC3810 were added.
12.0(7)XK	The **voice-encap** keyword for the Cisco MC3810 was removed. This keyword is no longer supported.
12.1(2)T	The **voice-encap** keyword for the Cisco MC3810 was removed. This keyword is no longer supported.
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.
12.0(33)S	Support for IPv6 was added. This command was implemented on the Cisco 12000 series routers.

Usage Guidelines

This command is typically used for subinterfaces; however, it can also be used on main interfaces. Using the **frame-relay interface-dlci** command on main interfaces will enable the use of routing protocols on interfaces that use Inverse ARP. The **frame-relay interface-dlci** command on a main interface is also valuable for assigning a specific class to a single PVC where special characteristics are desired. Subinterfaces are logical interfaces associated with a physical interface. You must specify the interface and subinterface before you can use this command to assign any DLCIs and any encapsulation or broadcast options.

A DLCI cannot be configured on a subinterface if the same DLCI has already been configured on the main interface. If the same DLCI is to be configured on the subinterface as on the main interface, the DLCI on the main interface must be removed first before it is configured on the subinterface. The DLCI on the main interface can be removed by using the **no frame-relay interface-dlci** command on the main interface.

This command is required for all point-to-point subinterfaces; it is also required for multipoint subinterfaces for which dynamic address resolution is enabled. It is not required for multipoint subinterfaces configured with static address mappings.

Use the **protocol ip** *ip-address* option only when this router or access server will act as the BOOTP server for auto installation over Frame Relay.

By issuing the **frame-relay interface-dlci** interface configuration command, you enter Frame Relay DLCI interface configuration mode (see the first example below). This gives you the following command options, which must be used with the relevant class or X.25-profile names you previously assigned:

- **class** *name*—Assigns a map class to a DLCI.
- **default**—Sets a command to its defaults.
- **no** {**class** *name* | **x25-profile** *name*}—Cancels the relevant class or X.25 profile.
- **x25-profile** *name*—Assigns an X.25 profile to a DLCI. (Annex G.)

A Frame Relay DLCI configured for Annex G can be thought of as a single logical X.25/LAPB interface. Therefore, any number of X.25 routes may be configured to route X.25 calls to that logical interface.

The **voice-cir** option on the Cisco MC3810 provides call admission control; it does not provide traffic shaping. A call setup will be refused if the unallocated bandwidth available at the time of the request is not at least equal to the value of the **voice-cir** option.

When configuring the **voice-cir** option on the Cisco MC3810 for Voice over Frame Relay, do not set the value of this option to be higher than the physical link speed. If Frame Relay traffic shaping is enabled for a PVC that is sharing voice and data, do not configure the **voice-cir** option to be higher than the value set with the **frame-relay mincir** command.

Note On the Cisco MC3810 only, the **voice-cir** option performs the same function as the **frame-relay voice bandwidth** map-class configuration command introduced in Cisco IOS Release 12.0(3)XG.

Examples

The following example assigns DLCI 100 to serial subinterface 5.17:

```
! Enter interface configuration and begin assignments on interface serial 5.
interface serial 5
! Enter subinterface configuration by assigning subinterface 17.
interface serial 5.17
! Now assign a DLCI number to subinterface 5.17.
frame-relay interface-dlci 100
```

The following example specifies DLCI 26 over serial subinterface 1.1 and assigns the characteristics under virtual-template 2 to this PPP connection:

```
Router(config)# interface serial1.1 point-to-point
Router(config-if)# frame-relay interface-dlci 26 ppp virtual-template2
```

The following example shows an Annex G connection being created by assigning the X.25 profile "NetworkNodeA" to Frame Relay DLCI interface 20 on serial interface 1 (having enabled Frame Relay encapsulation on that interface):

```
Router(config)# interface serial 1
Router(config-if)# encapsulation frame-relay
Router(config-if)# frame-relay interface-dlci 20
Router(config-fr-dlci)# x25-profile NetworkNodeA
```

The following example assigns DLCI 100 to serial subinterface 5.17:

```
Router(config)# interface serial 5
Router(config-if)# interface serial 5.17
Router(config-if)# frame-relay interface-dlci 100
```

The following example assigns DLCI 80 to the main interface first and then removes it before assigning the same DLCI to the subinterface. The DLCI must be removed from the main interface first, because the same dlci cannot be assigned to the subinterface after already being assigned to the main interface:

```
Router(config)# interface serial 2/0
Router(config-if)# encapsulation frame-relay
Router(config-if)# frame-relay interface-dlci 80
Router(config-fr-dlci)# exit
Router(config-if)# interface serial 2/0
Router(config-if)# no frame-relay interface-dlci 80
Router(config-if)# interface serial 2/0.1
Router(config-subif)# frame-relay interface-dlci 80
```

Related Commands

Command	Description
frame-relay class	Associates a map class with an interface or subinterface.
show frame-relay pvc	Displays statistics about PVCs for Frame Relay interfaces.
show interface	Displays P1024B/C information.
vofr	Configures subchannels and enables Voice over Frame Relay for a specific DLCI.

frame-relay intf-type

To configure a Frame Relay switch type, use the **frame-relay intf-type** command in interface configuration mode. To disable the switch, use the **no** form of this command.

frame-relay intf-type [**dce** | **dte** | **nni**]

no frame-relay intf-type [**dce** | **dte** | **nni**]

Syntax Description

dce	(Optional) Router or access server functions as a switch connected to a router.
dte	(Optional) Router or access server is connected to a Frame Relay network.
nni	(Optional) Router or access server functions as a switch connected to a switch—supports Network-to-Network Interface (NNI) connections.

Defaults

The router or access server is connected to a Frame Relay network.

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 12.2(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.
12.0(33)S	Support for IPv6 was added. This command was implemented on the Cisco 12000 series routers.

Usage Guidelines

This command can be used only if Frame Relay switching has previously been enabled globally by means of the **frame-relay switching** command.

Examples

The following example configures a DTE switch type:

```
frame-relay switching
!
interface serial 2
 frame-relay intf-type dte
```

frame-relay map ipv6

To define the mapping between a destination IPv6 address and the data-link connection identifier (DLCI) used to connect to the destination address, use the **frame-relay map ipv6** command in interface configuration mode. To delete the map entry, use the **no** form of this command.

frame-relay map ipv6 *ipv6-address dlci* [**broadcast**] [**cisco**] [**ietf**] [**payload-compression** {**packet-by-packet** | **frf9 stac** [*hardware-options*] | **data-stream stac** [*hardware-options*]}]

no frame-relay map ipv6 *ipv6-address*

Syntax Description

ipv6-address	Destination IPv6 (protocol) address that is being mapped to a permanent virtual circuit (PVC). This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
dlci	DLCI number used to connect to the specified protocol address on the interface. The acceptable range is from 16 to 1007.
broadcast	(Optional) Forwards IPv6 multicast packets to this address when multicast is not enabled (see the **frame-relay multicast-dlci** command for more information about multicasts). **Note** IPv6 supports multicast packets; broadcast packets are not supported.
cisco	(Optional) Cisco encapsulation method.
ietf	(Optional) Internet Engineering Task Force (IETF) Frame Relay encapsulation method. Used when the router or access server is connected to the equipment of another vendor across a Frame Relay network.
payload-compression	(Optional) Enables payload compression.
packet-by-packet	(Optional) Packet-by-packet payload compression using the Stacker method.
frf9 stac	(Optional) FRF.9 compression using the Stacker method: • If the router contains a compression service adapter (CSA), compression is performed in the CSA hardware (hardware compression). • If the CSA is not available, compression is performed in the software installed on the Versatile Interface Processor (VIP2) (distributed compression). • If the second-generation VIP2 is not available, compression is performed in the main processor of the router (software compression).

data-stream stac	(Optional) Data-stream compression using the Stacker method: • If the router contains a CSA, compression is performed in the CSA hardware (hardware compression). • If the CSA is not available, compression is performed in the main processor of the router (software compression).
hardware-options	(Optional) Choose one of the following hardware options: • **distributed**—Specifies that compression is implemented in the software that is installed in the VIP2. If the VIP2 is not available, compression is performed in the main processor of the router (software compression). This option applies only to the Cisco 7500 series routers. This option is not supported with data-stream compression. • **software**—Specifies that compression is implemented in the Cisco IOS software installed in the main processor of the router. • **csa** *csa-number*—Specifies the CSA to use for a particular interface. This option applies only to Cisco 7200 series routers.

Command Default

No mapping is defined.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)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 Release 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 introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The **frame-relay map ipv6** command is similar to the **frame-relay map** command, except that it is IPv6-specific.

Many DLCIs can be known by a router or access server and can send data to many different places, but they are all multiplexed over one physical link. The Frame Relay map defines the logical connection between a specific protocol and address pair and the correct DLCI.

The optional **ietf** and **cisco** keywords allow flexibility in the configuration. If no keywords are specified, the map inherits the attributes set with the **encapsulation frame-relay** command. You can also use the encapsulation options to specify that, for example, all interfaces use IETF encapsulation except one, which needs the original Cisco encapsulation method and can be configured through use of the **cisco** keyword with the **frame-relay map ipv6** command.

Data-stream compression is supported on interfaces and virtual circuits (VCs) using Cisco proprietary encapsulation. When the **data-stream stac** keywords are specified, Cisco encapsulation is automatically enabled. FRF.9 compression is supported on IETF-encapsulated VCs and interfaces. When the **frf9 stac** keywords are specified, IETF encapsulation is automatically enabled.

Packet-by-packet compression is Cisco-proprietary and will not interoperate with routers of other manufacturers.

You can disable payload compression by entering the **no frame-relay map ipv6 payload-compression** command and then entering the **frame-relay map ipv6** command again with one of the other encapsulation keywords (**ietf** or **cisco**).

Use the **frame-relay map ipv6** command to enable or disable payload compression on multipoint interfaces. Use the **frame-relay payload-compression** command to enable or disable payload compression on point-to-point interfaces.

We recommend that you shut down the interface before changing encapsulation types. Although not required, shutting down the interface ensures that the interface is reset for the new encapsulation.

Examples

In the following example, three nodes named Cisco A, Cisco B, and Cisco C make up a fully meshed network. Each node is configured with two PVCs, which provide an individual connection to each of the other two nodes. Each PVC is configured on a different point-to-point subinterface, which creates three unique IPv6 networks (2001:0DB8:2222:1017::/64, 2001:0DB8:2222:1018::/64, and 2001:0DB8:2222:1019::/64). Therefore, the mappings between the IPv6 addresses of each node and the DLCI (DLCI 17, 18, and 19) of the PVC used to reach the addresses are implicit (no additional mappings are required).

Note Given that each PVC in the following example is configured on a different point-to-point subinterface, the configuration in the following example can also be used in a network that is not fully meshed. Additionally, configuring each PVC on a different point-to-point subinterface can help simplify your routing protocol configuration. However, the configuration in the following example requires more than one IPv6 network, whereas configuring each PVC on point-to-multipoint interfaces requires only one IPv6 network.

Cisco A Configuration

```
interface Serial3
 encapsulation frame-relay
!
interface Serial3.17 point-to-point
 description to Cisco B
 ipv6 address 2001:0DB8:2222:1017::46/64
 frame-relay interface-dlci 17
!
interface Serial3.19 point-to-point
 description to Cisco C
 ipv6 address 2001:0DB8:2222:1019::46/64
 frame-relay interface-dlci 19
```

Cisco B Configuration

```
interface Serial5
 encapsulation frame-relay
!
interface Serial5.17 point-to-point
 description to Cisco A
 ipv6 address 2001:0DB8:2222:1017::73/64
 frame-relay interface-dlci 17
!
interface Serial5.18 point-to-point
 description to Cisco C
 ipv6 address 2001:0DB8:2222:1018::73/64
 frame-relay interface-dlci 18
```

Cisco C Configuration

```
interface Serial0
 encapsulation frame-relay
!
interface Serial0.18 point-to-point
 description to Cisco B
 ipv6 address 2001:0DB8:2222:1018::72/64
 frame-relay interface-dlci 18
!
interface Serial0.19 point-to-point
 description to Cisco A
 ipv6 address 2001:0DB8:2222:1019::72/64
 frame-relay interface-dlci 19
```

In the following example, the same three nodes (Cisco A, Cisco B, and Cisco C) from the previous example make up a fully meshed network and each node is configured with two PVCs (which provide an individual connection to each of the other two nodes). However, the two PVCs on each node in the following example are configured on a single interface (serial 3, serial 5, and serial 10, respectively), which makes each interface a point-to-multipoint interface. Therefore, explicit mappings are required between the link-local and global IPv6 addresses of each interface on all three nodes and the DLCI (DLCI 17, 18, and 19) of the PVC used to reach the addresses.

Cisco A Configuration

```
interface Serial3
 encapsulation frame-relay
 ipv6 address 2001:0DB8:2222:1044::46/64
 frame-relay map ipv6 FE80::E0:F727:E400:A 17 broadcast
 frame-relay map ipv6 FE80::60:3E47:AC8:8 19 broadcast
 frame-relay map ipv6 2001:0DB8:2222:1044::72 19
 frame-relay map ipv6 2001:0DB8:2222:1044::73 17
```

Cisco B Configuration

```
interface Serial5
 encapsulation frame-relay
 ipv6 address 2001:0DB8:2222:1044::73/64
 frame-relay map ipv6 FE80::60:3E59:DA78:C 17 broadcast
 frame-relay map ipv6 FE80::60:3E47:AC8:8 18 broadcast
 frame-relay map ipv6 2001:0DB8:2222:1044::46 17
 frame-relay map ipv6 2001:0DB8:2222:1044::72 18
```

Cisco C Configuration

```
interface Serial0
 encapsulation frame-relay
 ipv6 address 2001:0DB8:2222:1044::72/64
 frame-relay map ipv6 FE80::60:3E59:DA78:C 19 broadcast
```

```
frame-relay map ipv6 FE80::E0:F727:E400:A 18 broadcast
frame-relay map ipv6 2001:0DB8:2222:1044::46 19
frame-relay map ipv6 2001:0DB8:2222:1044::73 18
```

Related Commands

Command	Description
encapsulation frame-relay	Enables Frame Relay encapsulation.
frame-relay payload-compress	Enables Stacker payload compression on a specified point-to-point interface or subinterface.

frame-relay multilink ack

To configure the number of seconds for which a bundle link will wait for a hello message acknowledgment before resending the hello message, use the **frame-relay multilink ack** command in interface configuration mode. To reset this parameter to the default setting, use the **no** form of this command.

frame-relay multilink ack *seconds*

no frame-relay multilink ack

Syntax Description

seconds	Number of seconds for which a bundle link will wait for a hello message acknowledgment before resending the hello message. Range: 1 to 10. Default: 4.

Command Default

The default acknowledgement interval is 4 seconds.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(17)S	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(24)S	This command was implemented on VIP-enabled Cisco 7500 series routers.
12.3(4)T	Support for this command on VIP-enabled Cisco 7500 series routers was integrated into Cisco IOS Release 12.3(4)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.
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.
12.0(33)S	Support for IPv6 was added. This command was implemented on the Cisco 12000 series routers.

Usage Guidelines

The **frame-relay multilink ack** command can be configured only on bundle link interfaces that have been associated with a bundle using the **encapsulation frame-relay mfr** command.

Both ends of a bundle link send out hello messages at regular intervals. When a peer device receives a hello message, it responds by sending an acknowledgment. This exchange of hello messages and acknowledgments serves as a keepalive mechanism for the link. If the bundle link sends a hello message but does not receive an acknowledgment, it will resend the hello message up to a configured maximum number of times. If the bundle link exhausts the maximum number of retries, the bundle link line protocol is considered down (nonoperational).

The **frame-relay multilink ack** command setting on the local router is independent of the setting on the peer device.

Examples

The following example shows how to configure the bundle link to wait 6 seconds before resending hello messages:

```
interface serial0
 encapsulation frame-relay mfr0
 frame-relay multilink ack 6
```

Related Commands

Command	Description
encapsulation frame-relay mfr	Creates a multilink Frame Relay bundle link and associates the link with a bundle.
frame-relay multilink bandwidth-class	Specifies the bandwidth class used to trigger activation or deactivation of the Frame Relay bundle.
frame-relay multilink hello	Configures the interval at which a bundle link will send out hello messages.
frame-relay multilink retry	Configures the maximum number of times that a bundle link will resend a hello message while waiting for an acknowledgment.

frame-relay multilink bid

To assign a bundle identification (BID) name to a multilink Frame Relay bundle, use the **frame-relay multilink bid** command in interface configuration mode. To reset the name to the default, use the **no** form of this command.

frame-relay multilink bid *name*

no frame-relay multilink bid

Syntax Description

name	Bundle identification (BID) name. The name can be up to 49 characters long. The default is "mfr" followed by the number assigned to the bundle using the **interface mfr** command; for example, "mfr0."

Command Default

The BID name is assigned automatically as "mfr" followed by the number assigned to the bundle.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(17)S	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(24)S	This command was implemented on VIP-enabled Cisco 7500 series routers.
12.3(4)T	Support for this command on VIP-enabled Cisco 7500 series routers was integrated into Cisco IOS Release 12.3(4)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.
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.
12.0(33)S	Support for IPv6 was added. This command was implemented on the Cisco 12000 series routers.

Usage Guidelines

This command can be entered only on the multilink Frame Relay bundle interface.

Note You can enter the **frame-relay multilink bid** command at any time without affecting the current state of the interface; however, the BID will not go into effect until the interface has gone from the down state to the up state. One way to bring the interface down and back up again is by using the **shutdown** and **no shutdown** commands in interface configuration mode.

Only one BID is allowed per bundle. A later entry of the **frame-relay multilink bid** command supersedes prior entries.

The local and peer BIDs do not have to be unique.

Examples

The following example shows how to assign a BID of "bundle1" to the multilink Frame Relay bundle. The previous BID for the bundle was "mfr0."

```
interface mfr0
 frame-relay multilink bid bundle1
```

Related Commands

Command	Description
frame-relay multilink lid	Assigns a LID name to a multilink Frame Relay bundle link.
interface mfr	Configures a multilink Frame Relay bundle interface.
show frame-relay multilink	Displays configuration information and statistics about multilink Frame Relay bundles and bundle links.
shutdown (interface)	Disables an interface.

frame-relay multilink hello

To configure the interval at which a bundle link will send out hello messages, use the **frame-relay multilink hello** command in interface configuration mode. To reset this value to the default setting, use the **no** form of this command.

frame-relay multilink hello *seconds*

no frame-relay multilink hello

Syntax Description

seconds	Interval, in seconds, at which a bundle link will send out hello messages. Range: 1 to 180. Default: 10.

Command Default

The interval is set at 10 seconds.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(17)S	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(24)S	This command was implemented on VIP-enabled Cisco 7500 series routers.
12.3(4)T	Support for this command on VIP-enabled Cisco 7500 series routers was integrated into Cisco IOS Release 12.3(4)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.
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.
12.0(33)S	Support for IPv6 was added. This command was implemented on the Cisco 12000 series routers.

Usage Guidelines

The **frame-relay multilink hello** command can be configured only on bundle link interfaces that have been associated with a bundle using the **encapsulation frame-relay mfr** command.

Both ends of a bundle link send out hello messages at regular intervals. When a peer device receives a hello message, it responds by sending an acknowledgment. This exchange of hello messages and acknowledgments serves as a keepalive mechanism for the link. If the bundle link sends a hello message but does not receive an acknowledgment, it will resend the hello message up to a configured maximum number of times. If the bundle link exhausts the maximum number of retries, the bundle link line protocol is considered down (nonoperational).

The setting of the hello message interval on the local router is independent of the setting on the peer device.

Examples

The following example shows how to configure a bundle link to send hello messages every 15 seconds:

```
interface serial0
 encapsulation frame-relay mfr0
 frame-relay multilink hello 15
```

Related Commands

Command	Description
encapsulation frame-relay mfr	Creates a multilink Frame Relay bundle link and associates the link with a bundle.
frame-relay multilink ack	Configures the number of seconds that a bundle link will wait for a hello message acknowledgment before resending the hello message.
frame-relay multilink retry	Configures the maximum number of times that a bundle link will resend a hello message while waiting for an acknowledgment.

frame-relay multilink lid

To assign a bundle link identification (LID) name to a multilink Frame Relay bundle link, use the **frame-relay multilink lid** command in interface configuration mode. To reset the name to the default, use the **no** form of this command.

frame-relay multilink lid *name*

no frame-relay multilink lid

Syntax Description

name	Bundle link identification (LID) name. The name can be up to 49 characters long. The default is the name of the physical interface.

Command Default

The name of the physical interface is used as the LID.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(17)S	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(24)S	This command was implemented on VIP-enabled Cisco 7500 series routers.
12.3(4)T	Support for this command on VIP-enabled Cisco 7500 series routers was integrated into Cisco IOS Release 12.3(4)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.
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.
12.0(33)S	Support for IPv6 was added. This command was implemented on the Cisco 12000 series routers.

Usage Guidelines

The **frame-relay multilink lid** command can be configured only on bundle link interfaces that have been associated with a bundle using the **encapsulation frame-relay mfr** command.

Note You can enter the **frame-relay multilink lid** command at any time without affecting the current state of the interface; however, the LID will not go into effect until the interface has gone from the down state to the up state. One way to bring the interface down and back up again is by using the **shutdown** and **no shutdown** commands in interface configuration mode.

The LID will be used to identify the bundle link to peer devices and to enable the devices to identify which bundle links are associated with which bundles. The LID can also be assigned when the bundle link is created by using the **encapsulation frame-relay mfr** command with the *name* argument. If the LID is not assigned, the default LID is the name of the physical interface.

The local and peer LIDs do not have to be unique.

Examples

The following example shows the LID named BL1 assigned to serial interface 0:

```
interface serial 0
 encapsulation frame-relay mfr0
 frame-relay multilink lid BL1
```

Related Commands

Command	Description
encapsulation frame-relay mfr	Creates a multilink Frame Relay bundle link and associates the link with a bundle.
frame-relay multilink bid	Assigns a BID name to a multilink Frame Relay bundle.
show frame-relay multilink	Displays configuration information and statistics about multilink Frame Relay bundles and bundle links.
shutdown (interface)	Disables an interface.

frame-relay switching

To enable permanent virtual switching (PVC) switching on a Frame Relay DCE device or a Network-to-Network Interface (NNI), use the **frame-relay switching** command in global configuration mode. To disable switching, use the **no** form of this command.

frame-relay switching

no frame-relay switching

Syntax Description

This command has no arguments or keywords.

Defaults

Switching is not enabled.

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(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2(33)SB	This command's behavior was modified and implemented on the Cisco 10000 series router for the PRE3 and PRE4.
12.0(33)S	Support for IPv6 was added. This command was implemented on the Cisco 12000 series routers.

Usage Guidelines

You must add this command to the configuration file before configuring the routes.

Cisco 10000 Series Router Usage Guidelines

In Cisco IOS Release 12.2(33)SB, you do not need to configure the **frame-relay switching** command when configuring a Frame Relay interface as the DCE.

In Cisco IOS Release 12.2(31)SB, you must configure the **frame-relay switching** command when you configure a Frame Relay interface as the DCE.

Examples

The following example shows the command that is entered in the configuration file before the Frame Relay configuration commands to enable switching:

```
frame-relay switching
```

glbp authentication

To configure an authentication string for the Gateway Load Balancing Protocol (GLBP), use the **glbp authentication** command in interface configuration mode. To disable authentication, use the **no** form of this command.

glbp *group-number* **authentication** {**text** *string* | **md5** {**key-string** [**0** | **7**] *key* | **key-chain** *name-of-chain*}}

no glbp *group-number* **authentication** {**text** *string* | **md5** {**key-string** [**0** | **7**] *key* | **key-chain** *name-of-chain*}}

Syntax Description

group-number	GLBP group number in the range from 0 to 1023.
text *string*	Specifies an authentication string. The number of characters in the command plus the text string must not exceed 255 characters.
md5	Message Digest 5 (MD5) authentication.
key-string *key*	Specifies the secret key for MD5 authentication. The key string cannot exceed 100 characters in length. We recommend using at least 16 characters.
0	(Optional) Unencrypted key. If no prefix is specified, the key is unencrypted.
7	(Optional) Encrypted key.
key-chain *name-of-chain*	Identifies a group of authentication keys.

Command Default

No authentication of GLBP messages occurs.

Command Modes

Interface configuration (config-if)

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.
12.3(2)T	The **md5** keyword and associated parameters were added.
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 same authentication method must be configured on all the routers that are configured to be members of the same GLBP group, to ensure interoperation. A router will ignore all GLBP messages that contain the wrong authentication information.

If password encryption is configured with the **service password-encryption** command, the software saves the key string in the configuration as encrypted text.

Examples

The following example configures stringxyz as the authentication string required to allow GLBP routers in group 10 to interoperate:

```
Router(config)# interface fastethernet 0/0
Router(config-if)# glbp 10 authentication text stringxyz
```

In the following example, GLBP queries the key chain "AuthenticateGLBP" to obtain the current live key and key ID for the specified key chain:

```
Router(config)# key chain AuthenticateGLBP
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string ThisIsASecretKey
Router(config-keychain-key)# key-string ThisIsASecretKey
Router(config-keychain-key)# exit
Router(config-keychain)# exit
Router(config)# interface Ethernet0/1
Router(config-if)# ip address 10.0.0.1 255.255.255.0
Router(config-if)# glbp 2 authentication md5 key-chain AuthenticateGLBP
```

Related Commands

Command	Description
glbp ip	Enables GLBP.
service password-encryption	Encrypts passwords.

glbp forwarder preempt

To configure a router to take over as active virtual forwarder (AVF) for a Gateway Load Balancing Protocol (GLBP) group if the current AVF falls below its low weighting threshold, use the **glbp forwarder preempt** command in interface configuration mode. To disable this function, use the **no** form of this command.

glbp *group* **forwarder preempt** [**delay minimum** *seconds*]

no glbp *group* **forwarder preempt** [**delay minimum**]

Syntax Description

group	GLBP group number in the range from 0 to 1023.
delay minimum *seconds*	(Optional) Specifies a minimum number of seconds that the router will delay before taking over the role of AVF. The range is from 0 to 3600 seconds with a default delay of 30 seconds.

Command Default

Forwarder preemption is enabled with a default delay of 30 seconds.

Command Modes

Interface configuration (config-if)

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.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Examples

The following example shows a router being configured to preempt the current AVF when the current AVF falls below its low weighting threshold. If the router preempts the current AVF, it waits 60 seconds before taking over the role of the AVF.

```
glbp 10 forwarder preempt delay minimum 60
```

Related Commands

Command	Description
glbp ip	Enables GLBP.

glbp ipv6

To activate the Gateway Load Balancing Protocol (GLBP) in IPv6, use the **glbp ipv6** command in interface configuration mode. To disable GLBP, use the **no** form of this command.

glbp *group* **ipv6** [*ipv6-address* | **autoconfig**]

no glbp *group* **ipv6** [*ipv6-address* | **autoconfig**]

Syntax Description

group	GLBP group number in the range from 0 to 1023.
ip-address	(Optional) Virtual IPv6 address for the GLBP group. The IPv6 address must be in the same subnet as the interface IPv6 address.
autoconfig	(Optional) Indicates a default IPv6 address can be created based on a MAC address.

Command Default

GLBP is disabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SXI	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

The **glbp ipv6** command activates GLBP on the configured interface. If an IPv6 address is specified, that address is used as the designated virtual IPv6 address for the GLBP group. If no IPv6 address is specified, the designated address is learned from another router configured to be in the same GLBP group. For GLBP to elect an active virtual gateway (AVG), at least one router on the cable must have been configured with the designated address. A router must be configured with, or have learned, the virtual IPv6 address of the GLBP group before assuming the role of a GLBP gateway or forwarder. Configuring the designated address on the AVG always overrides a designated address that is in use.

When the **glbp ipv6** command is enabled on an interface, the handling of proxy Address Resolution Protocol (ARP) requests is changed (unless proxy ARP was disabled). ARP requests are sent by hosts to map an IPv6 address to a MAC address. The GLBP gateway intercepts the ARP requests and replies to the ARP on behalf of the connected nodes. If a forwarder in the GLBP group is active, proxy ARP requests are answered using the MAC address of the first active forwarder in the group. If no forwarder is active, proxy ARP responses are suppressed.

Examples

The following example enables GLBP on an IPv6 configured interface:

```
Router(config-if)# glbp ipv6
```

Related Commands

Command	Description
glbp ip	Activates the GLBP in IPv4.
show glbp	Displays GLBP information.

glbp load-balancing

To specify the load-balancing method used by the active virtual gateway (AVG) of the Gateway Load Balancing Protocol (GLBP), use the **glbp load-balancing** command in interface configuration mode. To disable load balancing, use the **no** form of this command.

glbp *group* **load-balancing** [**host-dependent** | **round-robin** | **weighted**]

no glbp *group* **load-balancing**

Syntax Description

group	GLBP group number in the range from 0 to 1023.
host-dependent	(Optional) Specifies a load balancing method based on the MAC address of a host where the same forwarder is always used for a particular host while the number of GLBP group members remains unchanged.
round-robin	(Optional) Specifies a load balancing method where each virtual forwarder in turn is included in address resolution replies for the virtual IP address. This method is the default.
weighted	(Optional) Specifies a load balancing method that is dependent on the weighting value advertised by the gateway.

Command Default

The round-robin method is the default.

Command Modes

Interface configuration (config-if)

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.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.4(24)T2	This command was modified. When the **no** form of this command is configured, if the AVG does not have an AVF, it preferentially replies to ARP requests with the MAC address of the first listening virtual forwarder.
15.0(1)M1	This command was modified. When the **no** form of this command is configured, if the AVG does not have an Active Virtual Forwarder (AVF), it preferentially replies to ARP requests with the MAC address of the first listening virtual forwarder.
15.1(2)T	This command was modified. When the **no** form of this command is configured, if the AVG does not have an AVF, it preferentially replies to ARP requests with the MAC address of the first listening virtual forwarder.

Usage Guidelines

Use the host-dependent method of GLBP load balancing when you need each host to always use the same router. Use the weighted method of GLBP load balancing when you need unequal load balancing because routers in the GLBP group have different forwarding capacities.

Examples

The following example shows the host-dependent load-balancing method being configured for the AVG of the GLBP group 10:

```
Router(config)# interface fastethernet 0/0
Router(config-if)# glbp 10 ip 10.21.8.10
Router(config-if)# glbp 10 load-balancing host-dependent
```

Related Commands

Command	Description
show glbp	Displays GLBP information.

glbp name

To enable IP redundancy by assigning a name to the Gateway Load Balancing Protocol (GLBP) group, use the **glbp name** command in interface configuration mode. To disable IP redundancy for a group, use the **no** form of this command.

glbp *group-number* **name** *group-name*

no glbp *group-number* **name** *group-name*

Syntax Description

group-number	GLBP group number. Range is from 0 to 1023.
group-name	GLBP group name specified as a character string. Maximum number of characters is 255.

Defaults

IP redundancy for a group is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(7)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 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

The GLBP redundancy client must be configured with the same GLBP group name so that the redundancy client and the GLBP group can be connected.

Examples

The following example assigns the abccomp name to GLBP group 10:

```
Router(config-if)# glbp 10 name abccomp
```

Related Commands

Command	Description
glbp authentication	Configures an authentication string for the GLBP.
glbp forwarder preempt	Configures a router to take over as AVF for a GLBP group if it has higher priority than the current AVF.
glbp ip	Activates GLBP.
glbp load-balancing	Specifies the load-balancing method used by the AVG of GLBP.

Command	Description
glbp preempt	Configures the gateway to take over as AVG for a GLBP group if it has higher priority than the current AVG.
glbp priority	Sets the priority level of the gateway within a GLBP group.
glbp timers	Configures the time between hello packets sent by the GLBP gateway and the time for which the virtual gateway and virtual forwarder information is considered valid.
glbp timers redirect	Configures the time during which the AVG for a GLBP group continues to redirect clients to a secondary AVF.
glbp weighting	Specifies the initial weighting value of the GLBP gateway.
glbp weighting track	Specifies a tracking object where the GLBP weighting changes based on the availability of the object being tracked.
show glbp	Displays GLBP information.
track	Configures an interface to be tracked where the GLBP weighting changes based on the state of the interface.

glbp preempt

To configure the gateway to take over as active virtual gateway (AVG) for a Gateway Load Balancing Protocol (GLBP) group if it has higher priority than the current AVG, use the **glbp preempt** command in interface configuration mode. To disable this function, use the **no** form of this command.

glbp *group* **preempt** [**delay minimum** *seconds*]

no glbp *group* **preempt** [**delay minimum**]

Syntax Description

group	GLBP group number in the range from 0 to 1023.
delay minimum *seconds*	(Optional) Specifies a minimum number of seconds that the router will delay before taking over the role of AVG. The range is from 0 to 3600 seconds with a default delay of 30 seconds.

Command Default

A GLBP router with a higher priority than the current AVG cannot assume the role of AVG.
The default delay value is 30 seconds.

Command Modes

Interface configuration (config-if)

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.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Examples

The following example shows a router being configured to preempt the current AVG when its priority of 254 is higher than that of the current AVG. If the router preempts the current AVG, it waits 60 seconds before assuming the role of AVG.

```
Router(config-if)# glbp 10 preempt delay minimum 60
Router(config-if)# glbp 10 priority 254
```

Related Commands

Command	Description
glbp ip	Enables GLBP.
glbp priority	Sets the priority level of the router within a GLBP group.

glbp priority

To set the priority level of the gateway within a Gateway Load Balancing Protocol (GLBP) group, use the **glbp priority** command in interface configuration mode. To remove the priority level of the gateway, use the **no** form of this command.

glbp *group* **priority** *level*

no glbp *group* **priority** *level*

Syntax Description

group	GLBP group number in the range from 0 to 1023.
level	Priority of the gateway within the GLBP group. The range is from 1 to 255. The default is 100.

Command Default

The GLBP virtual gateway preemptive scheme is disabled

Command Modes

Interface configuration (config-if)

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

Use this command to control which virtual gateway becomes the active virtual gateway (AVG). After the priorities of several different virtual gateways are compared, the gateway with the numerically higher priority is elected as the AVG. If two virtual gateways have equal priority, the gateway with the higher IP address is selected.

Examples

The following example shows a virtual gateway being configured with a priority of 254:

```
Router(config-if)# glbp 10 priority 254
```

Related Commands

Command	Description
glbp ip	Enables GLBP.
glbp preempt	Configures a router to take over as the AVG for a GLBP group if it has higher priority than the current AVG.

glbp timers

To configure the time between hello packets sent by the Gateway Load Balancing Protocol (GLBP) gateway and the time that the virtual gateway and virtual forwarder information is considered valid, use the **glbp timers** command in interface configuration mode. To restore the timers to their default values, use the **no** form of this command.

glbp *group* **timers** [**msec**] *hellotime* [**msec**] *holdtime*

no glbp *group* **timers**

Syntax Description

group	GLBP group number in the range from 0 to 1023.
msec	(Optional) Specifies that the following (*hellotime* or *holdtime)* argument value will be expressed in milliseconds rather than seconds.
hellotime	Hello interval. The default is 3 seconds (3000 milliseconds).
holdtime	Time before the virtual gateway and virtual forwarder information contained in the hello packet is considered invalid. The default is 10 seconds (10,000 milliseconds).

Command Default

GLBP timers are set to their default values.

Command Modes

Interface configuration (config-if)

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.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

Routers on which timer values are not configured can learn timer values from the active virtual gateway (AVG). The timers configured on the AVG always override any other timer settings. All routers in a GLBP group should use the same timer values. If a GLBP gateway sends a hello message, the information should be considered valid for one holdtime. Normally, holdtime is greater than three times the value of hello time, (*holdtime* > 3 * *hellotime*). The range of values for holdtime force the holdtime to be greater than the hello time.

Examples

The following example shows the GLBP group 10 on Fast Ethernet interface 0/0 timers being configured for an interval of 5 seconds between hello packets, and the time after which virtual gateway and virtual forwarder information is considered to be invalid to 18 seconds:

```
Router(config)# interface fastethernet 0/0
Router(config-if)# glbp 10 ip
Router(config-if)# glbp 10 timers 5 18
```

Related Commands

Command	Description
glbp ip	Activates GLBP.
show glbp	Displays GLBP information.

glbp timers redirect

To configure the time during which the active virtual gateway (AVG) for a Gateway Load Balancing Protocol (GLBP) group continues to redirect clients to a secondary active virtual forwarder (AVF), use the **glbp timers redirect** command in interface configuration mode. To restore the redirect timers to their default values, use the **no** form of this command.

glbp *group* **timers redirect** *redirect timeout*

no glbp *group* **timers redirect** *redirect timeout*

Syntax Description

group	GLBP group number in the range from 0 to 1023.
redirect	The redirect timer interval in the range from 0 to 3600 seconds. The default is 600 seconds (10 minutes). **Note** The zero value for the *redirect* argument cannot be removed from the range of acceptable values because preexisting configurations of Cisco IOS software already using the zero value could be negatively affected during an upgrade. However, be advised that a zero setting is not recommended and, if used, results in a redirect timer that never expires. If the redirect timer does not expire, then when a router fails, new hosts continue to be assigned to the failed router instead of being redirected to the backup.
timeout	The time interval, in the range from 600 to 64,800 seconds, before the secondary virtual forwarder becomes unavailable. The default is 14,400 seconds (4 hours).

Command Default

The GLBP redirect timers are set to their default values.

Command Modes

Interface configuration (config-if)

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.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

A virtual forwarder that is assigned a virtual MAC address by the AVG is known as a primary virtual forwarder. If the virtual forwarder has learned the virtual MAC address from hello messages, it is referred to as a secondary virtual forwarder.

The redirect timer sets the time delay between a forwarder failing on the network and the AVG assuming that the forwarder will not return. The virtual MAC address to which the forwarder was responsible for replying is still given out in Address Resolution Protocol (ARP) replies, but the forwarding task is handled by another router in the GLBP group.

Note The zero value for the *redirect* argument cannot be removed from the range of acceptable values because preexisting configurations of Cisco IOS software already using the zero value could be negatively affected during an upgrade. However, be advised that a zero setting is not recommended and, if used, results in a redirect timer that never expires. If the redirect timer does not expire, then when a router fails, new hosts continue to be assigned to the failed router instead of being redirected to the backup.

The timeout interval is the time delay between a forwarder failing on the network and the MAC address for which the forwarder was responsible becoming inactive on all of the routers in the GLBP group. After the timeout interval, packets sent to this virtual MAC address will be lost. The timeout interval must be long enough to allow all hosts to refresh their ARP cache entry that contained the virtual MAC address.

Examples

The following example shows the commands used to configure GLBP group 1 on Fast Ethernet interface 0/0 with a redirect timer of 1800 seconds (30 minutes) and timeout interval of 28,800 seconds (8 hours):

```
Router# config terminal
Router(config)# interface fastEthernet 0/0
Router(config-if)# glbp 1 timers redirect 1800 28800
```

glbp weighting

To specify the initial weighting value of the Gateway Load Balancing Protocol (GLBP) gateway, use the **glbp weighting** command in interface configuration mode. To restore the default values, use the **no** form of this command.

glbp *group* **weighting** *maximum* [**lower** *lower*] [**upper** *upper*]

no glbp *group* **weighting**

Syntax Description

group	GLBP group number in the range from 0 to 1023.
maximum	Maximum weighting value in the range from 1 to 254. Default value is 100.
lower *lower*	(Optional) Specifies a lower weighting value in the range from 1 to the specified maximum weighting value. Default value is 1.
upper *upper*	(Optional) Specifies an upper weighting value in the range from the lower weighting to the maximum weighting value. The default value is the specified maximum weighting value.

Command Default

The default gateway weighting value is 100 and the default lower weighting value is 1.

Command Modes

Interface configuration (config-if)

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.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

The weighting value of a virtual gateway is a measure of the forwarding capacity of the gateway. If a tracked interface on the router fails, the weighting value of the router may fall from the maximum value to below the lower threshold, causing the router to give up its role as a virtual forwarder. When the weighting value of the router rises above the upper threshold, the router can resume its active virtual forwarder role.

Use the **glbp weighting track** and **track** commands to configure parameters for an interface to be tracked. If an interface on a router goes down, the weighting for the router can be reduced by a specified value.

Examples

The following example shows the weighting of the gateway for GLBP group 10 being set to a maximum of 110 with a lower weighting limit of 95 and an upper weighting limit of 105:

```
Router(config)# interface fastethernet 0/0
Router(config-if)# ip address 10.21.8.32 255.255.255.0
Router(config-if)# glbp 10 weighting 110 lower 95 upper 105
```

Related Commands

Command	Description
glbp weighting track	Specifies an object to be tracked that affects the weighting of a GLBP gateway.
track	Configures an interface to be tracked.

glbp weighting track

To specify a tracking object where the Gateway Load Balancing Protocol (GLBP) weighting changes based on the availability of the object being tracked, use the **glbp weighting track** command in interface configuration mode. To remove the tracking, use the **no** form of this command.

glbp *group* **weighting track** *object-number* [**decrement** *value*]

no glbp *group* **weighting track** *object-number* [**decrement** *value*]

Syntax Description

group	GLBP group number in the range from 0 to 1023.
object-number	Object number representing an item to be tracked. The valid range is 1 to 1000. Use the **track** command to configure the tracked object.
decrement *value*	(Optional) Specifies an amount by which the GLBP weighting for the router is decremented (or incremented) when the interface goes down (or comes back up). The value range is from 1 to 254, with a default value of 10.

Command Default

Objects are not tracked for GLBP weighting changes.

Command Modes

Interface configuration (config-if)

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.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.1(3)T	This command was modified. The valid range for the *object-number* argument increased to 1000.
15.1(1)S	This command was modified. The valid range for the *object-number* argument increased to 1000.

Usage Guidelines

This command ties the weighting of the GLBP gateway to the availability of its interfaces. It is useful for tracking interfaces that are not configured for GLBP.

When a tracked interface goes down, the GLBP gateway weighting decreases by 10. If an interface is not tracked, its state changes do not affect the GLBP gateway weighting. For each GLBP group, you can configure a separate list of interfaces to be tracked.

The optional *value* argument specifies by how much to decrement the GLBP gateway weighting when a tracked interface goes down. When the tracked interface comes back up, the weighting is incremented by the same amount.

When multiple tracked interfaces are down, the configured weighting decrements are cumulative.

Use the **track** command to configure each interface to be tracked.

As of Cisco IOS Release 15.1(3)T, a maximum of 1000 objects can be tracked. Although 1000 tracked objects can be configured, each tracked object uses CPU resources. The amount of available CPU resources on a router is dependent upon variables such as traffic load and how other protocols are configured and run. The ability to use 1000 tracked objects is dependent upon the available CPU. Testing should be conducted on site to ensure that the service works under the specific site traffic conditions.

Examples

In the following example, Fast Ethernet interface 0/0 tracks two interfaces represented by the numbers 1 and 2. If interface 1 goes down, the GLBP gateway weighting decreases by the default value of 10. If interface 2 goes down, the GLBP gateway weighting decreases by 5.

```
Router(config)# interface fastethernet 0/0
Router(config-if)# ip address 10.21.8.32 255.255.255.0
Router(config-if)# glbp 10 weighting track 1
Router(config-if)# glbp 10 weighting track 2 decrement 5
```

Related Commands

Command	Description
glbp weighting	Specifies the initial weighting value of a GLBP gateway.
track	Configures an interface to be tracked.

graceful-restart

To enable the Open Shortest Path First version 3 (OSPFv3) graceful restart feature on a graceful-restart-capable router, use the **graceful-restart** command in OSPF router configuration mode. To disable graceful restart, use the **no** form of this command.

graceful-restart [**restart-interval** *interval*]

no graceful-restart

Syntax Description

restart-interval *interval*	(Optional) Graceful-restart interval in seconds. The range is from 1 to 1800, and the default is 120.

Command Default

The GR feature is not enabled on GR-capable routers.

Command Modes

OSPFv3 router configuration mode (config-router)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 12.5(1)M.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.
15.1(3)S	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.
Cisco IOS XE Release 3.4S	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.
15.2(1)T	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.

Usage Guidelines

The **graceful-restart** command can be enabled only on GR-capable routers.

Examples

The following examples enables graceful restart mode on a GR-capable router in IPv6 and IPv4:

```
Router(config)# ospfv3 router 1
Router(config-router)# graceful-restar
```

The following examples enables graceful restart mode on a GR-capable router in IPv6 only:

```
Router(config)# ipv6 router ospf 1234
Router(config-router)# graceful-restart
```

Related commands

Command	Description
graceful-restart helper	Enables the OSPFv3 graceful restart feature on a GR-aware router.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

graceful-restart helper

To enable the Open Shortest Path First version 3 (OSPFv3) graceful restart feature on a graceful-restart-aware router, use the **graceful-restart helper** command in OSPFv3 router configuration mode. To reset the router to its default, use the **no** form of this command.

graceful-restart helper {**disable** | **strict-lsa-checking**}

no graceful-restart helper

Syntax Description

disable	Disables graceful-restart-aware mode.
strict-lsa-checking	Enables graceful restart-helper mode with strict link-state advertisement (LSA) checking.

Command Default

Graceful restart-aware mode is enabled.

Command Modes

OSPFv3 router configuration mode (config-router)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 12.5(1)M.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.
15.1(3)S	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process. The **disable** and **strict-lsa-checking** keywords can be used only in an IPv6 OSPFv3 process.
Cisco IOS XE Release 3.4S	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process. The **disable** and **strict-lsa-checking** keywords can be used only in an IPv6 OSPFv3 process.
15.2(1)T	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process. The **disable** and **strict-lsa-checking** keywords can be used only in an IPv6 OSPFv3 process.

Usage Guidelines

GR-helper mode is configurable on both GR-aware and GR-capable routers; however, GR-aware routers can use only the **graceful-restart helper** command.

The **strict-lsa-checking** keyword indicates whether an OSPFv3 GR-aware router should terminate the helper function when there is a change to an LSA that would be flooded to the restarting router or when there is a changed LSA on the restarting router's retransmission list when graceful restart is initiated.

Examples

The following example enables GR-helper mode with strict LSA checking:

```
Router(config)# ipv6 router ospf 1234
Router(config-router)# graceful-restart helper strict-lsa-checking
```

The following example shows how to enable GR-helper mode in an OSPFv3 IPv4 instance:

```
Router(config)# ospfv3 router 1
Router(config-router)# graceful-restart helper
```

Related Commands

Command	Description
graceful-restart	Enables the OSPFv3 GR feature on a graceful-restart-capable router.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

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.

hardware statistics

To enable the collection of hardware statistics, use the **hardware statistics** command in IPv6or IPv4 access-list configuration mode. To disable this feature, use the **no** form of this command.

hardware statistics

no hardware statistics

Syntax Description

This commands has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

IPv6 access-list configuration (config-ipv6-acl)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

The hardware statistics command affects only global access-list (ACL) counters.

Examples

The following example enables the collection of hardware statistics in an IPv6 configuration:

```
Router(config-ipv6-acl)# hardware statistics
```

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.

home-address

To specify the mobile router home address using an IPv6 address or interface identifier, use the **home-address** command in IPv6 mobile router configuration mode. To disable this function, use the **no** form of this command.

home-address {**home-network** | *ipv6-address-identifier* | *interface*}

no home-address

Syntax Description

home-network	Specifies the home network's IPv6 prefix on the mobile router.
ipv6-address-identifier	The IPv6 home address identifier.
interface	Specifies the interface to use to identify the home address.

Command Default

No IPv6 home address is specified.

Command Modes

IPv6 mobile router configuration (IPv6-mobile-router)

Command History

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

Usage Guidelines

The **home-address** command allows you to specify the IPv6 home address. When multiple home networks have been configured, we recommend that you use the **home-address home-network** command syntax, so that the mobile router builds a home address that matches the home network to which it registers.

Examples

The following example shows multiple configured home networks and enables the mobile router to build a home address that matches its registered home network:

```
Router(config)# ipv6 mobile router
Router(IPv6-mobile-router)# eui-interface Ethernet0/0
Router(IPv6-mobile-router)# home-network 2001:0DB8:1/64 priority 18
Router(IPv6-mobile-router)# home-network 2001:0DB8:2/64
Router(IPv6-mobile-router)# home-network 2001:0DB8:3/64 discover
Router(IPv6-mobile-router)# home-network 2001:0DB8:4/64 priority 200
Router(IPv6-mobile-router)# home-address home-network eui-64
```

Related Commands

Command	Description
home-network	Specifies the home network's IPv6 prefix on the mobile router.
ipv6 mobile router	Enables IPv6 NEMO functionality on the router and places the router in IPv6 mobile router mode.

home-network

To specify the home network's IPv6 prefix on the mobile router, use the **home-network** command in IPv6 mobile router configuration mode. To disable this function, use the **no** form of this command.

home-network *ipv6-prefix*

no home-network

Syntax Description

ipv6-prefix	The IPv6 prefix of the home network.

Command Default

The IPv6 home network prefix is not specified.

Command Modes

IPv6 mobile router configuration (IPv6-mobile-router)

Command History

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

Usage Guidelines

Users can configure up to 10 home-network entries, and they are used in order of priority. The prefix identifies the home network of the mobile router and is used to discover when the mobile router is at home.

When multiple home networks have been configured, we recommend that you use the **home-address home-network** command syntax, so that the mobile router builds a home address that matches the home network to which it registers.

The command syntax sorts the home networks by priority. The default priority is 128. The home networks will be tried from the smaller to the higher value and, for a same priority, the addresses without the discover keyword are tried first.

Examples

The following example shows multiple configured home networks and enables the mobile router to build a home address that matches its registered home network:

```
Router(config)# ipv6 mobile router
Router(IPv6-mobile-router)# eui-interface Ethernet0/0
Router(IPv6-mobile-router)# home-network 2001:0DB8:1/64 priority 18
Router(IPv6-mobile-router)# home-network 2001:0DB8:2/64
Router(IPv6-mobile-router)# home-network 2001:0DB8:3/64 discover
Router(IPv6-mobile-router)# home-network 2001:0DB8:4/64 priority 200
Router(IPv6-mobile-router)# home-address home-network eui-64
```

Related Commands

Command	Description
home-address	Specifies the mobile router home address using an IPv6 address or interface identifier.
ipv6 mobile router	Enables IPv6 NEMO functionality on the router and places the router in IPv6 mobile router mode.

hop-limit

To verify the advertised hop-count limit, use the **hop-limit** command in router advertisement (RA) guard policy configuration mode.

hop-limit {**maximum** *limit* | **minimum** *limit*}

Syntax Description

maximum *limit*	Verifies that the hop-count limit is greater than that set by the *limit* argument.
minimum *limit*	Verifies that the hop-count limit is less than that set by the *limit* argument.

Command Default

No hop-count limit is specified.

Command Modes

RA guard policy configuration (config-ra-guard)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

The **hop-limit** command enables verification that the advertised hop-count limit is greater than or less than the value set by the *limit* argument. Configuring the **minimum** *limit* keyword and argument can prevent an attacker from setting a low hop-count limit value on the hosts to block them from generating traffic to remote destinations; that is, beyond their default router. If the advertised hop-count limit value is unspecified (which is the same as setting a value of 0), the packet is dropped.

Configuring **maximum** *limit* keyword and argument enables verification that the advertised hop-count limit is lower than the value set by the *limit* argument. If the advertised hop-count limit value is unspecified (which is the same as setting a value of 0), the packet is dropped.

Examples

The following example defines an RA guard policy name as raguard1, places the router in RA guard policy configuration mode, and sets a minimum hop-count limit of 3:

```
Router(config)# ipv6 nd raguard policy raguard1
Router(config-ra-guard)# hop-limit minimum 3
```

Related Commands

Command	Description
ipv6 nd raguard policy	Defines the RA guard policy name and enters RA guard policy configuration mode.

host group

To create a host group configuration in IPv6 Mobile, use the **host group** command in home agent configuration mode. To remove a host configuration, use the **no** form of this command.

host group *profile-name*

no host group *profile-name*

Syntax Description

profile-name	Specifies a name for the host group.

Command Default

No IPv6 Mobile host configurations exist.

Command Modes

Home agent configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

The **host group** command creates an IPv6 Mobile home-agent host configuration with a given profile name. Multiple instances with different profile names can be created and used.

Do not configure two separate groups with the same IPv6 address. For example, host group group1 and host group group2 cannot both be configured with the same IPv6 address of baba::1.

Examples

In the following example, the user enters home agent configuration mode and creates a host group named group1:

```
Router(config)# ipv6 mobile home-agent
Router(config-ha)# host group group1
```

Related Commands

Command	Description
address (IPv6 mobile router)	Specifies the home address of the IPv6 Mobile node.
ipv6 mobile home-agent (global configuration)	Enters home agent configuration mode.
nai	Specifies the NAI for the IPv6 mobile node.

hostname

To specify or modify the hostname for the network server, use the **hostname** command in global configuration mode.

hostname *name*

Syntax Description

name	New hostname for the network server.

Command Default

The default hostname is Router.

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.
12.2(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.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.0(1)M4	This command was integrated into Cisco IOS Release 15.0(1)M4 and support for numeric hostnames added.

Usage Guidelines

The hostname is used in prompts and default configuration filenames.

Do not expect case to be preserved. Uppercase and lowercase characters look the same to many internet software applications. It may seem appropriate to capitalize a name the same way you might do in English, but conventions dictate that computer names appear all lowercase. For more information, refer to RFC 1178, *Choosing a Name for Your Computer.*

The name must also follow the rules for ARPANET hostnames. They must start with a letter, end with a letter or digit, and have as interior characters only letters, digits, and hyphens. Names must be 63 characters or fewer. Creating an all numeric hostname is not recommended but the name will be accepted after an error is returned.

```
Router(config)#hostname 123
% Hostname contains one or more illegal characters.
123(config)#
```

A hostname of less than 10 characters is recommended. For more information, refer to RFC 1035, *Domain Names—Implementation and Specification*.

On most systems, a field of 30 characters is used for the hostname and the prompt in the CLI. Note that the length of your hostname may cause longer configuration mode prompts to be truncated. For example, the full prompt for service profile configuration mode is:

```
(config-service-profile)#
```

However, if you are using the hostname of “Router,” you will only see the following prompt (on most systems):

```
Router(config-service-profil)#
```

If the hostname is longer, you will see even less of the prompt:

```
Basement-rtr2(config-service)#
```

Keep this behavior in mind when assigning a name to your system (using the **hostname** global configuration command). If you expect that users will be relying on mode prompts as a CLI navigation aid, you should assign hostnames of no more than nine characters.

The use of a special character such as '\'(backslash) and a three or more digit number for the character setting like **hostname**, results in incorrect translation:

```
Router(config)#
Router(config)#hostname \99
% Hostname contains one or more illegal characters.
```

Examples

The following example changes the hostname to “host1”:

```
Router(config)# hostname host1
host1(config)#
```

Related Commands

Command	Description
setup	Enables you to make major changes to your configurations, for example, adding a protocol suit, making major addressing scheme changes, or configuring newly installed interfaces.

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** *email-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 *email-id*	Uses the e-mail ID to identify the peer.
key-id *key-id*	Uses the proprietary 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 e-mail ID, 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 an 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 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.

import dns-server

To import the Domain Name System (DNS) recursive name server option to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **import dns-server** command in IPv6 DHCP pool configuration mode. To remove the available DNS recursive name server list, use the **no** form of this command.

import dns-server

no import dns-server

Syntax Description

This command has no arguments or keywords.

Command Default

The DNS recursive name server list is not imported to a client.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

DHCP for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The DNS recursive name server option provides a list of one or more IPv6 addresses of DNS recursive name servers to which a client's DNS resolver may send DNS queries. The DNS servers are listed in the order of preference for use by the client resolver.

The DNS recursive name server list option code is 23. For more information on DHCP options and suboptions, see the "DHCP Options" appendix in the *Network Registrar User's Guide*, Release 6.2.

Examples

The following example shows how to import a list of available DNS recursive name servers to a client:

```
Router(config-dhcp)# import dns-server
```

Related Commands

Command	Description
import domain-name	Imports the domain search list option to a DHCP for IPv6 client.

import domain-name

To import the domain name search list option to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **import domain-name** command in IPv6 DHCP pool configuration mode. To remove the domain name search list, use the **no** form of this command.

import domain-name

no import domain-name

Syntax Description

This command has no arguments or keywords.

Command Default

The domain search list is not imported to the client.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

DHCP for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The domain name search list option specifies the domain search list the client is to use when resolving hostnames with DNS.

The domain name search list option code is 24. For more information on DHCP options and suboptions, see the "DHCP Options" appendix in the *Network Registrar User's Guide*, Release 6.2.

Examples

The following example shows how to import a domain search list to the client:

```
Router(config-dhcp)# import domain-name
```

Related Commands

Command	Description
import dns-server	Imports the DNS recursive name server option to a DHCP for IPv6 client.

import information refresh

To import the information refresh time option to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **import information refresh** command in IPv6 DHCP pool configuration mode. To remove the specified refresh time, use the **no** form of this command.

import information refresh

no import information refresh

Syntax Description

This command has no arguments or keywords.

Command Default

The information refresh time option is not imported.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

DHCP for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The information refresh time option specifies an upper bound for how long a client should wait before refreshing information retrieved from DHCP for IPv6. It is used only in Reply messages in response to Information Request messages. In other messages, there will usually be other options that indicate when the client should contact the server (for example, addresses with lifetimes).

The information refresh time option code is 32. For more information on DHCP options and suboptions, see the “DHCP Options” appendix in the *Network Registrar User's Guide*, Release 6.2.

Examples

The following example shows how to import the information refresh time:

```
import information refresh
```

Related Commands

Command	Description
information refresh	Specifies the information refresh time to be sent to the client.

import nis address

To import the network information service (NIS) address option to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **import nis address** command in IPv6 DHCP pool configuration mode. To remove the NIS address, use the **no** form of this command.

import nis address

no import nis address

Syntax Description

This command has no arguments or keywords.

Command Default

No NIS address is imported.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

DHCP for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The NIS servers option provides a list of one or more IPv6 addresses of NIS servers available to send to the client. The client must view the list of NIS servers as an ordered list, and the server may list the NIS servers in the order of the server's preference.

The NIS servers option code is 27. For more information on DHCP options and suboptions, see the "DHCPv6 Options" appendix in the *Network Registrar User's Guide*, Release 6.2.

Examples

The following example shows how to import the NIS address of an IPv6 server:

```
import nis address
```

Related Commands

Command	Description
import nis domain	Imports the NIS domain name option to a DHCP for IPv6 client.

Command	Description
nis address	Specifies the NIS address of an IPv6 server to be sent to the client.
nis domain-name	Enables a server to convey a client's NIS domain name information to the client.

import nisp domain-name

To import the network information service plus (NIS+) domain name option to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **import nisp domain-name** command in IPv6 DHCP pool configuration mode. To remove the domain name, use the **no** form of this command.

import nisp domain-name

no import nisp domain-name

Syntax Description

This command has no arguments or keywords.

Command Default

No NIS+ domain name is specified.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

DHCP for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The NIS+ domain name option provides an NIS+ domain name for the client.

The NIS+ domain name option code is 30. For more information on DHCP options and suboptions, see the “DHCPv6 Options” appendix in the *Network Registrar User's Guide*, Release 6.2.

Examples

The following example shows how to import the NIS+ domain name of a client:

```
import nisp domain-name
```

Related Commands

Command	Description
import nisp address	Imports the NIS+ server option to a DHCP for IPv6 client.
nisp address	Specifies the NIS+ address of an IPv6 server to be sent to the client.
nisp domain-name	Enables a server to convey a client’s NIS+ domain name information to the client.

import nisp address

To import the network information service plus (NIS+) servers option to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **import nisp address** command in IPv6 DHCP pool configuration mode. To remove the NIS address, use the **no** form of this command.

import nisp address

no import nisp address

Syntax Description

This command has no arguments or keywords.

Command Default

No NIS+ address is imported.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

DHCP for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The NIS+ servers option provides a list of one or more IPv6 addresses of NIS+ servers available to send to the client. The client must view the list of NIS+ servers as an ordered list, and the server may list the NIS+ servers in the order of the server's preference.

The NIS+ servers option code is 28. For more information on DHCP options and suboptions, see the "DHCPv6 Options" appendix in the *Network Registrar User's Guide*, Release 6.2.

Examples

The following example shows how to import the NIS+ address of an IPv6 server:

```
import nisp address
```

Related Commands

Command	Description
import nisp domain	Imports the NIS+ domain name option to a DHCP for IPv6 client.

Command	Description
nisp address	Specifies the NIS+ address of an IPv6 server to be sent to the client.
nisp domain-name	Enables a server to convey a client's NIS+ domain name information to the client.

import nisp domain-name

To import the network information service plus (NIS+) domain name option to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **import nisp domain-name** command in IPv6 DHCP pool configuration mode. To remove the domain name, use the **no** form of this command.

import nisp domain-name

no import nisp domain-name

Syntax Description

This command has no arguments or keywords.

Command Default

No NIS+ domain name is specified.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

DHCP for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The NIS+ domain name option provides an NIS+ domain name for the client.

The NIS+ domain name option code is 30. For more information on DHCP options and suboptions, see the "DHCPv6 Options" appendix in the *Network Registrar User's Guide*, Release 6.2.

Examples

The following example shows how to import the NIS+ domain name of a client:

```
import nisp domain-name
```

Related Commands

Command	Description
import nisp address	Imports the NIS+ server option to a DHCP for IPv6 client.
nisp address	Specifies the NIS+ address of an IPv6 server to be sent to the client.
nisp domain-name	Enables a server to convey a client's NIS+ domain name information to the client.

import sip address

To import the Session Initiation Protocol (SIP) server IPv6 address list option to the outbound SIP proxy server, use the **import sip address** command in IPv6 DHCP pool configuration mode. To remove the SIP server IPv6 address list, use the **no** form of this command.

import sip address

no import sip address

Syntax Description

This command has no arguments or keywords.

Command Default

SIP IPv6 address list is not imported.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

Dynamic Host Configuration Protocol (DHCP) for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

A SIP server is the host on which the outbound SIP proxy server is running.

The SIP server IPv6 address list option specifies a list of IPv6 addresses that indicate SIP outbound proxy servers available to the client. Servers must be listed in order of preference.

The SIP server IPv6 address list option code is 22. For more information on DHCP options and suboptions, see the “DHCP Options” appendix in the *Network Registrar User's Guide*, Release 6.2.

Examples

The following example enables the user to import a SIP server IPv6 address list to the client:

```
Router(config-dhcp)# import sip address
```

Related Commands

Command	Description
import sip domain-name	Imports a SIP server domain-name list option to the outbound SIP proxy server.

import sip domain-name

To import a Session Initiation Protocol (SIP) server domain-name list option to the outbound SIP proxy server, use the **import sip domain-name** command in IPv6 DHCP pool configuration mode. To remove the SIP server domain-name list, use the **no** form of this command.

import sip domain-name

no import sip domain-name

Syntax Description

This command has no arguments or keywords.

Command Default

SIP domain-name list is not imported.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

Dynamic Host Configuration Protocol (DHCP) for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

A SIP server is the host on which the outbound SIP proxy server is running.

The SIP server domain-name list option contains the domain names of the SIP outbound proxy servers. Domain names must be listed in order of preference. The option may contain multiple domain names, but the client must try the records in the order listed. The client resolves the subsequent domain names only if attempts to contact the first one failed or yielded no common transport protocols between client and server or denoted a domain administratively prohibited by client policy.

The SIP server domain-name list option code is 21. For more information on DHCP options and suboptions, see the “DHCP Options” appendix in the *Network Registrar User's Guide*, Release 6.2.

Examples

The following example enables the user to import a SIP server domain-name list to the client:

```
Router(config-dhcp)# import sip domain-name
```

Related Commands

Command	Description
import sip address	Imports the SIP server IPv6 address list option to the outbound SIP proxy server.

import sntp address

To import the Simple Network Time Protocol (SNTP) address option to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **import sntp address** command in IPv6 DHCP pool configuration mode. To remove the SNTP server address, use the **no** form of the command.

import sntp address *ipv6-address*

no import sntp address *ipv6-address*

Syntax Description

ipv6-address	(Optional) The IPv6 address for SNTP. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

Command Default

No SNTP server address is imported.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

DHCP for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The SNTP server option provides a list of one or more IPv6 addresses of SNTP servers available to the client for synchronization. The clients use these SNTP servers to synchronize their system time to that of the standard time servers.

Clients must treat the list of SNTP servers as an ordered list, and the server may list the SNTP servers in decreasing order of preference. The SNTP address option can be used only to configure information about SNTP servers that can be reached using IPv6.

The SNTP server option code is 31. For more information on DHCP options and suboptions, see the "DHCP Options" appendix in the *Network Registrar User's Guide*, Release 6.2.

Examples

The following example shows how to import the SNTP server address:

```
import sntp address
```

Related Commands

Command	Description
sntp address	Specifies the SNTP server to be sent to the client.

information refresh

To specify the information refresh time to be sent to the client, use the **information refresh** command in IPv6 DHCP pool configuration mode. To remove the specified refresh time, use the **no** form of this command.

information refresh {*days* [*hours minutes*] | **infinity**}

no information refresh {*days* [*hours minutes*] | **infinity**}

Syntax Description

days	Refresh time specified in number of days. The default is 0 0 86400, which equals 24 hours.
hours	(Optional) Refresh time specified in number of hours.
minutes	(Optional) Refresh time specified in number of minutes. The minimum refresh time that can be used is 0 0 600, which is 10 minutes.
infinity	Sets the IPv6 value of 0xffffffff used to configure the information refresh time to infinity.

Command Default

Information refresh information is not sent to the client. The client refreshes every 24 hours if no refresh information is sent.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

Dynamic Host Configuration Protocol (DHCP) for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The information refresh time option specifies the maximum time a client should wait before refreshing information retrieved from DHCP for IPv6. It is only used in Reply messages in response to Information Request messages. In other messages, there will usually be other options that indicate when the client should contact the server (for example, addresses with lifetimes).

The maximum value for the information refresh period on the DHCP for IPv6 client is 7 days. The maximum value is not configurable.

The information refresh time option code is 32. For more information on DHCP options and suboptions, see the “DHCP Options” appendix in the *Network Registrar User's Guide*, Release 6.2.

Examples

The following example shows how to specify the information refresh time to be 1 day, 1 hour, and 1 second:

```
information refresh 1 1 1
```

Related Commands

Command	Description
import information refresh	Imports the information refresh time option to a DHCP for IPv6 client.

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.
15.1(2)T	Support for IPv6 was added.

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.

interface mfr

To configure a multilink Frame Relay bundle interface, use the **interface mfr** command in global configuration mode. To remove the bundle interface, use the **no** form of this command.

interface mfr *number*

no interface mfr *number*

Syntax Description

number	Number that will uniquely identify this bundle interface. Range: 0 to 2147483647.

Command Default

A Frame Relay bundle interface is not configured.

Command Modes

Global configuration

Command History

Release	Modification
12.0(17)S	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(24)S	This command was introduced on VIP-enabled Cisco 7500 series routers.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(4)T	Support for this command on VIP-enabled Cisco 7500 series routers was 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.
12.2SX	This command is supported in the Cisco 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

Frame Relay encapsulation is the default encapsulation type for multilink Frame Relay bundle interfaces.

A bundle interface is a virtual interface that serves as the Frame Relay data link and performs the same functions as a physical interface. The bundle is made up of physical serial links, called bundle links. The bundle links within a bundle function as one physical link and one pool of bandwidth. Functionality that you want to apply to the bundle links must be configured on the bundle interface.

The **no interface mfr** command will work only if all bundle links have been removed from the bundle by using the **no encapsulation frame-relay mfr** command.

Examples

The following example shows the configuration of a bundle interface called “mfr0.” The bundle identification (BID) name “BUNDLE-A” is assigned to the bundle. Serial interfaces 0 and 1 are assigned to the bundle as bundle links.

```
interface mfr0
 frame-relay multilink bid BUNDLE-A
!
interface serial0
 encapsulation frame-relay mfr0
!
interface serial1
 encapsulation frame-relay mfr0
```

Related Commands

Command	Description
debug frame-relay multilink	Displays debug messages for multilink Frame Relay bundles and bundle links.
encapsulation frame-relay mfr	Creates a multilink Frame Relay bundle link and associates the link with a bundle.
frame-relay multilink bandwidth-class	Specifies the bandwidth class used to trigger activation or deactivation of the Frame Relay bundle.
frame-relay multilink bid	Assigns a BID name to a multilink Frame Relay bundle.
show frame-relay multilink	Displays configuration information and statistics about multilink Frame Relay bundles and bundle links.

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* [**type** *virtual-template-type*]

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.
type *virtual-template-type*	(Optional) Specifies the type of virtual template.

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.
Cisco IOS XE Release 2.5	This command was implemented on Cisco ASR 1000 series routers.

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 address

To set a primary or secondary IP address for an interface, use the **ip address** command in interface configuration mode. To remove an IP address or disable IP processing, use the **no** form of this command.

ip address *ip-address mask* [**secondary** [**vrf** *vrf-name*]]

no ip address *ip-address mask* [**secondary** [**vrf** *vrf-name*]]

Syntax Description

ip-address	IP address.
mask	Mask for the associated IP subnet.
secondary	(Optional) Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address. **Note** If the secondary address is used for a VRF table configuration with the **vrf** keyword, the **vrf** keyword must be specified also.
vrf	(Optional) Name of the VRF table. The *vrf-name* argument specifies the VRF name of the ingress interface.

Command Default

No IP address is defined for the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
10.0	This command was introduced.
12.2(28)SB	The **vrf** keyword and *vrf-name* argument were introduced.
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)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SCB	This command was integrated into Cisco IOS Release 12.2(33)SCB.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.1(1)S	This command was integrated into Cisco IOS Release 15.1(1)S.

Usage Guidelines

An interface can have one primary IP address and multiple secondary IP addresses. Packets generated by the Cisco IOS software always use the primary IP address. Therefore, all routers and access servers on a segment should share the same primary network number.

Hosts can determine subnet masks using the Internet Control Message Protocol (ICMP) mask request message. Routers respond to this request with an ICMP mask reply message.

You can disable IP processing on a particular interface by removing its IP address with the **no ip address** command. If the software detects another host using one of its IP addresses, it will print an error message on the console.

The optional **secondary** keyword allows you to specify an unlimited number of secondary addresses. Secondary addresses are treated like primary addresses, except the system never generates datagrams other than routing updates with secondary source addresses. IP broadcasts and Address Resolution Protocol (ARP) requests are handled properly, as are interface routes in the IP routing table.

Secondary IP addresses can be used in a variety of situations. The following are the most common applications:

- There may not be enough host addresses for a particular network segment. For example, your subnetting allows up to 254 hosts per logical subnet, but on one physical subnet you need 300 host addresses. Using secondary IP addresses on the routers or access servers allows you to have two logical subnets using one physical subnet.
- Many older networks were built using Level 2 bridges. The judicious use of secondary addresses can aid in the transition to a subnetted, router-based network. Routers on an older, bridged segment can be easily made aware that many subnets are on that segment.
- Two subnets of a single network might otherwise be separated by another network. This situation is not permitted when subnets are in use. In these instances, the first network is *extended*, or layered on top of the second network using secondary addresses.

Note If any router on a network segment uses a secondary address, all other devices on that same segment must also use a secondary address from the same network or subnet. Inconsistent use of secondary addresses on a network segment can very quickly cause routing loops.

Note When you are routing using the Open Shortest Path First (OSPF) algorithm, ensure that all secondary addresses of an interface fall into the same OSPF area as the primary addresses.

To transparently bridge IP on an interface, you must perform the following two tasks:

- Disable IP routing (specify the **no ip routing** command).
- Add the interface to a bridge group, see the **bridge-group** command.

To concurrently route and transparently bridge IP on an interface, see the **bridge crb** command.

Examples

In the following example, 192.108.1.27 is the primary address and 192.31.7.17 and 192.31.8.17 are secondary addresses for Ethernet interface 0:

```
interface ethernet 0
 ip address 192.108.1.27 255.255.255.0
 ip address 192.31.7.17 255.255.255.0 secondary
 ip address 192.31.8.17 255.255.255.0 secondary
```

In the following example, Ethernet interface 0/1 is configured to automatically classify the source IP address in the VRF table vrf1:

```
interface ethernet 0/1
 ip address 10.108.1.27 255.255.255.0
 ip address 10.31.7.17 255.255.255.0 secondary vrf vrf1
 ip vrf autoclassify source
```

Related Commands

Command	Description
bridge crb	Enables the Cisco IOS software to both route and bridge a given protocol on separate interfaces within a single router.
bridge-group	Assigns each network interface to a bridge group.
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 ip interface	Displays the usability status of interfaces configured for IP.
show route-map	Displays static and dynamic route maps.

ip directed-broadcast

To enable the translation of a directed broadcast to physical broadcasts, use the **ip directed-broadcast** interface configuration command. To disable this function, use the **no** form of this command.

ip directed-broadcast [*access-list-number* | *extended access-list-number*]

no ip directed-broadcast [*access-list-number* | *extended access-list-number*]

Syntax Description

access-list-number	(Optional) Standard access list number in the range from 1 to 199. If specified, a broadcast must pass the access list to be forwarded.
extended access-list-number	(Optional) Extended access list number in the range from 1300 to 2699.

Command Default

Disabled; all IP directed broadcasts are dropped.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
10.0	This command was introduced.
12.0	The default behavior changed to directed broadcasts being dropped.
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

An IP directed broadcast is an IP packet whose destination address is a valid broadcast address for some IP subnet, but which originates from a node that is not itself part of that destination subnet.

A router that is not directly connected to its destination subnet forwards an IP directed broadcast in the same way it would forward unicast IP packets destined to a host on that subnet. When a directed broadcast packet reaches a router that is directly connected to its destination subnet, that packet is "exploded" as a broadcast on the destination subnet. The destination address in the IP header of the packet is rewritten to the configured IP broadcast address for the subnet, and the packet is sent as a link-layer broadcast.

The **ip directed-broadcast** command controls the explosion of directed broadcasts when they reach their target subnets. The command affects only the final transmission of the directed broadcast on its ultimate destination subnet. It does not affect the transit unicast routing of IP directed broadcasts.

If **directed broadcast** is enabled for an interface, incoming IP packets whose addresses identify them as directed broadcasts intended for the subnet to which that interface is attached will be exploded as broadcasts on that subnet. If an access list has been configured with the **ip directed-broadcast** command, only directed broadcasts that are permitted by the access list in question will be forwarded; all other directed broadcasts destined for the interface subnet will be dropped.

If the **no ip directed-broadcast** command has been configured for an interface, directed broadcasts destined for the subnet to which that interface is attached will be dropped, rather than being broadcast.

Note Because directed broadcasts, and particularly Internet Control Message Protocol (ICMP) directed broadcasts, have been abused by malicious persons, we recommend that security-conscious users disable the **ip directed-broadcast** command on any interface where directed broadcasts are not needed and that they use access lists to limit the number of exploded packets.

Examples

The following example enables forwarding of IP directed broadcasts on Ethernet interface 0:

```
Router(config)# interface ethernet 0
Router(config-if)# ip directed-broadcast
```

Related Commands

Command	Description
ip forward-protocol	Specifies which protocols and ports the router forwards when forwarding broadcast packets.

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 server

To enable the HTTP server on your IP or IPv6 system, including the Cisco web browser user interface, use the **ip http server** command in global configuration mode. To disable the HTTP server, use the **no** form of this command.

ip http server

no ip http server

Syntax Description

This command has no arguments or keywords.

Command Default

The HTTP server is disabled on the Cisco Catalyst 4000 series switch. The HTTP server is enabled for clustering on the following Cisco switches: Catalyst 3700 series, Catalyst 3750 series, Catalyst 3550 series, Catalyst 3560 series, and Catalyst 2950 series.

The HTTP server uses the standard port 80 by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2	This command was introduced.
12.2(2)T	IPv6 support was added.
12.2(15)T	The HTTP 1.0 implementation was replaced by the HTTP 1.1 implementation. The secure HTTP server feature was added.
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.
12.2SX	This command is supported in the Cisco 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.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
12.4(24)T	Support for IPv6 Secure Neighbor Discovery (SeND) was added.

Usage Guidelines

With IPv6 support added in Cisco IOS Release 12.2(2)T, the **ip http server** command simultaneously enables and disables both IP and IPv6 access to the HTTP server. However, an access list configured with the **ip http access-class** command will only be applied to IPv4 traffic. IPv6 traffic filtering is not supported.

Caution The standard HTTP server and the secure HTTP (HTTPS) server can run on a system at the same time. If you enable the HTTPS server using the **ip http secure-server** command, disable the standard HTTP server using the **no ip http server** command to ensure that secure data cannot be accessed through the standard HTTP connection.

Examples

The following example shows how to enable the HTTP server on both IP and IPv6 systems:

```
Router(config)# ip http server
Router(config)# ip http path flash:
```

Related Commands

Command	Description
ip http access-class	Specifies the access list that should be used to restrict access to the HTTP server.
ip http path	Specifies the base path used to locate files for use by the HTTP server.
ip http secure-server	Enables the HTTPS server.

ip mroute-cache

Note Effective with Cisco IOS Release 15.0(1)M and Cisco IOS Release 12.2(33)SRE, the **ip mroute-cache** command is not available in Cisco IOS software.

To configure IP multicast fast switching or multicast distributed switching (MDS), use the **ip mroute-cache** command in interface configuration mode. To disable either of these features, use the **no** form of this command.

ip mroute-cache [**distributed**]

no ip mroute-cache [**distributed**]

Syntax Description

distributed	(Optional) Enables MDS on the interface. In the case of Cisco 7500 series routers, this keyword is optional; if it is omitted, fast switching occurs. On the Cisco 12000 series, this keyword is required because the Cisco 12000 series does only distributed switching.

Command Default

On the Cisco 7500 series, IP multicast fast switching is enabled; MDS is disabled.
On the Cisco 12000 series, MDS is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
11.2(11)GS	The **distributed** 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.
12.0(33)S	Support for IPv6 was added. This command was implemented on the Cisco 12000 series routers.
15.0(1)M	This command was removed.
12.2(33)SRE	This command was removed.

Usage Guidelines

On the Cisco 7500 Series

If multicast fast switching is disabled on an incoming interface for a multicast routing table entry, the packet will be sent at the process level for all interfaces in the outgoing interface list.

If multicast fast switching is disabled on an outgoing interface for a multicast routing table entry, the packet is process-level switched for that interface, but may be fast switched for other interfaces in the outgoing interface list.

When multicast fast switching is enabled (like unicast routing), debug messages are not logged. If you want to log debug messages, disable fast switching.

If MDS is not enabled on an incoming interface that is capable of MDS, incoming multicast packets will not be distributed switched; they will be fast switched at the Route Processor (RP). Also, if the incoming interface is not capable of MDS, packets will get fast switched or process switched at the RP.

If MDS is enabled on the incoming interface, but at least one of the outgoing interfaces cannot fast switch, packets will be process switched. We recommend that you disable fast switching on any interface when MDS is enabled.

On the Cisco 12000 Series

On the Cisco 12000 series router, all interfaces should be configured for MDS because that is the only switching mode.

Examples

The following example shows how to enable IP multicast fast switching on the interface:

```
ip mroute-cache
```

The following example shows how to disable IP multicast fast switching on the interface:

```
no ip mroute-cache
```

The following example shows how to enable MDS on the interface:

```
ip mroute-cache distributed
```

The following example shows how to disable MDS and IP multicast fast switching on the interface:

```
no ip mroute-cache distributed
```

ip name-server

To specify the address of one or more name servers to use for name and address resolution, use the **ip name-server** command in global configuration mode. To remove the addresses specified, use the **no** form of this command.

ip name-server [**vrf** *vrf-name*] *server-address1* [*server-address2...server-address6*]

no ip name-server [**vrf** *vrf-name*] *server-address1* [*server-address2...server-address6*]

Syntax Description

vrf *vrf-name*	(Optional) Defines a Virtual Private Network (VPN) routing and forwarding instance (VRF) table. The *vrf-name* argument specifies a name for the VRF table.
server-address1	IPv4 or IPv6 addresses of a name server.
server-address2...server-address6	(Optional) IP addresses of additional name servers (a maximum of six name servers).

Command Default

No name server addresses are specified.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(2)T	Support for IPv6 addresses was added.
12.0(21)ST	Support for IPv6 addresses was added.
12.0(22)S	Support for IPv6 addresses was added.
12.2(14)S	Support for IPv6 addresses was 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.
12.4(4)T	The **vrf** keyword and *vrf-name* argument were added.
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 introduced on Cisco ASR 1000 Series Routers.

Examples

The following example shows how to specify IPv4 hosts 172.16.1.111 and 172.16.1.2 as the name servers:

```
ip name-server 172.16.1.111 172.16.1.2
```

This command will be reflected in the configuration file as follows:

```
ip name-server 172.16.1.111
```

```
ip name-server 172.16.1.2
```

The following example shows how to specify IPv4 hosts 172.16.1.111 and 172.16.1.2 as the name servers for vpn1:

```
Router(config)# ip name-server vrf vpn1 172.16.1.111 172.16.1.2
```

The following example shows how to specify IPv6 hosts 3FFE:C00::250:8BFF:FEE8:F800 and 2001:0DB8::3 as the name servers:

```
ip name-server 3FFE:C00::250:8BFF:FEE8:F800 2001:0DB8::3
```

This command will be reflected in the configuration file as follows:

```
ip name-server 3FFE:C00::250:8BFF:FEE8:F800
ip name-server 2001:0DB8::3
```

Related Commands

Command	Description
ip domain-lookup	Enables the IP DNS-based hostname-to-address translation.
ip domain-name	Defines a default domain name to complete unqualified hostnames (names without a dotted decimal domain name).

ip route-cache

To control the use of switching methods for forwarding IP packets, use the **ip route-cache** command in interface configuration mode. To disable any of these switching methods, use the **no** form of this command.

ip route-cache [**cef | distributed | flow | policy | same-interface**]

no ip route-cache [**cef | distributed | flow | policy | same-interface**]

Syntax Description

cef	(Optional) Enables Cisco Express Forwarding operation on an interface.
distributed	(Optional) Enables distributed switching on the interface. (This keyword is not supported on the Cisco 7600 routers.) Distributed switching is disabled by default.
flow	(Optional) Enables NetFlow accounting for packets that are received by the interface. The default is disabled.
policy	(Optional) Enables fast-switching for packets that are forwarded using policy-based routing (PBR). Fast Switching for PBR (FSPBR) is disabled by default.
same-interface	(Optional) Enables fast-switching of packets onto the same interface on which they arrived.

Command Default

The switching method is not controlled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
10.0	This command was introduced.
11.1	The **flow** keyword was added.
11.2GS	The **cef** and **distributed** keywords were added.
11.1CC	**cef** keyword support was added for multiple platforms.
12.0	The **policy** keyword was added.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S. The **ip route-cache flow** command is automatically remapped to the **ip flow ingress** command.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB. This command is not supported on the Cisco 10000 series router.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

IP Route Cache

Note The Cisco 10000 series routers do *not* support the **ip route-cache** command.

Using the route cache is often called *fast switching*. The route cache allows outgoing packets to be load-balanced on a *per-destination* basis rather than on a per-packet basis. The **ip route-cache** command with no additional keywords enables fast switching.

Entering the **ip route-cache** command has no effect on a subinterface. Subinterfaces accept the **no** form of the command; however, this disables Cisco Express Forwarding or distributed Cisco Express Forwarding on the physical interface and all subinterfaces associated with the physical interface

The default behavior for Fast Switching varies by interface and media.

Note IPv4 fast switching is removed with the implementation of the Cisco Express Forwarding infrastructure enhancements for Cisco IOS 12.2(25)S-based releases and Cisco IOS Release 12.4(20)T. For these and later Cisco IOS releases, switching path are Cisco Express Forwarding switched or process switched.

IP Route Cache Same Interface

You can enable IP fast switching when the input and output interfaces are the same interface, using the **ip route-cache same-interface** command. This configuration normally is not recommended, although it is useful when you have partially meshed media, such as Frame Relay or you are running Web Cache Communication Protocol (WCCP) redirection. You could use this feature on other interfaces, although it is not recommended because it would interfere with redirection of packets to the optimal path.

IP Route Cache Flow

The flow caching option can be used in conjunction with Cisco Express Forwarding switching to enable NetFlow, which allows statistics to be gathered with a finer granularity. The statistics include IP subprotocols, well-known ports, total flows, average number of packets per flow, and average flow lifetime.

Note The **ip route-cache flow** command has the same functionality as the **ip flow ingress** command, which is the preferred command for enabling NetFlow. If either the **ip route-cache flow** command or the **ip flow ingress** command is configured, both commands will appear in the output of the **show running-config** command.

IP Route Cache Distributed

The distributed option is supported on Cisco routers with line cards and Versatile Interface Processors (VIPs) that support Cisco Express Forwarding switching.

On Cisco routers with Route/Switch Processor (RSP) and VIP controllers, the VIP hardware can be configured to switch packets received by the VIP with no per-packet intervention on the part of the RSP. When VIP distributed switching is enabled, the input VIP interface tries to switch IP packets instead of forwarding them to the RSP for switching. Distributed switching helps decrease the demand on the RSP.

If the **ip route-cache distributed**, **ip cef distributed**, and **ip route-cache flow** commands are configured, the VIP performs distributed Cisco Express Forwarding switching and collects a finer granularity of flow statistics.

IP Route-Cache Cisco Express Forwarding

In some instances, you might want to disable Cisco Express Forwarding or distributed Cisco Express Forwarding on a particular interface because that interface is configured with a feature that Cisco Express Forwarding or distributed Cisco Express Forwarding does not support. Because all interfaces that support Cisco Express Forwarding or distributed Cisco Express Forwarding are enabled by default when you enable Cisco Express Forwarding or distributed Cisco Express Forwarding operation globally, you must use the **no** form of the **ip route-cache distributed** command in the interface configuration mode to turn Cisco Express Forwarding or distributed Cisco Express Forwarding operation off a particular interface.

Disabling Cisco Express Forwarding or distributed Cisco Express Forwarding on an interface disables Cisco Express Forwarding or distributed Cisco Express Forwarding switching for packets forwarded to the interface, but does not affect packets forwarded out of the interface.

Additionally, when you disable distributed Cisco Express Forwarding on the RSP, Cisco IOS software switches packets using the next-fastest switch path (Cisco Express Forwarding).

Enabling Cisco Express Forwarding globally disables distributed Cisco Express Forwarding on all interfaces. Disabling Cisco Express Forwarding or distributed Cisco Express Forwarding globally enables process switching on all interfaces.

Note On the Cisco 12000 series Internet router, you must not disable distributed Cisco Express Forwarding on an interface.

IP Route Cache Policy

If Cisco Express Forwarding is already enabled, the **ip route-cache route** command is not required because PBR packets are Cisco Express Forwarding-switched by default.

Before you can enable fast-switched PBR, you must first configure PBR.

FSPBR supports all of PBR's **match** commands and most of PBR's **set** commands, with the following restrictions:

- The **set ip default next-hop** and **set default interface** commands are not supported.
- The **set interface** command is supported only over point-to-point links, unless a route cache entry exists using the same interface specified in the **set interface** command in the route map. Also, at the process level, the routing table is consulted to determine if the interface is on a reasonable path to the destination. During fast switching, the software does not make this check. Instead, if the packet matches, the software blindly forwards the packet to the specified interface.

Note Not all switching methods are available on all platforms. Refer to the *Cisco Product Catalog* for information about features available on the platform you are using.

Examples

Configuring Fast Switching and Disabling Cisco Express Forwarding Switching

The following example shows how to enable fast switching and disable Cisco Express Forwarding switching:

```
Router(config)# interface ethernet 0/0/0
Router(config-if)# ip route-cache
```

The following example shows that fast switching is enabled:

```
Router# show ip interface fastEthernet 0/0/0
```

```
FastEthernet0/0/0 is up, line protocol is up
  Internet address is 10.1.1.254/24
  Broadcast address is 255.255.255.224
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  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 Distributed switching is disabled
  IP Feature Fast switching turbo vector
  IP Null turbo vector
  IP multicast fast switching is enabled
```

The following example shows that Cisco Express Forwarding switching is disabled:

```
Router# show cef interface fastEthernet 0/0/0

FastEthernet0/0/0 is up (if_number 3)
  Corresponding hwidb fast_if_number 3
  Corresponding hwidb firstsw->if_number 3
  Internet address is 10.1.1.254/24
  ICMP redirects are always sent
  Per packet load-sharing is disabled
  IP unicast RPF check is disabled
  Inbound access list is not set
  Outbound access list is not set
  IP policy routing is disabled
  Hardware idb is FastEthernet0/0/0
  Fast switching type 1, interface type 18
  IP CEF switching disabled
  IP Feature Fast switching turbo vector
  IP Null turbo vector
  Input fast flags 0x0, Output fast flags 0x0
  ifindex 1(1)
  Slot 0 Slot unit 0 VC -1
  Transmit limit accumulator 0x48001A02 (0x48001A02)
  IP MTU 1500
```

The following example shows the configuration information for FastEthernet interface 0/0/0:

```
Router# show running-config
.
.
!
interface FastEthernet0/0/0
 ip address 10.1.1.254 255.255.255.0
 no ip route-cache cef
 no ip route-cache distributed
!
```

The following example shows how to enable Cisco Express Forwarding (and to disable distributed Cisco Express Forwarding if it is enabled):

```
Router(config-if)# ip route-cache cef
```

The following example shows how to enable VIP distributed Cisco Express Forwarding and per-flow accounting on an interface (regardless of the previous switching type enabled on the interface):

```
Router(config)# interface e0
Router(config-if)# ip address 10.252.245.2 255.255.255.0
Router(config-if)# ip route-cache distributed
Router(config-if)# ip route-cache flow
```

The following example shows how to enable Cisco Express Forwarding on the router globally (which also disables distributed Cisco Express Forwarding on any interfaces that are running distributed Cisco Express Forwarding), and disable Cisco Express Forwarding (which enables process switching) on Ethernet interface 0:

```
Router(config)# ip cef
Router(config)# interface e0
Router(config-if)# no ip route-cache cef
```

The following example shows how to enable distributed Cisco Express Forwarding operation on the router (globally), and disable Cisco Express Forwarding operation on Ethernet interface 0:

```
Router(config)# ip cef distributed
Router(config)# interface e0
Router(config-if)# no ip route-cache cef
```

The following example shows how to reenable distributed Cisco Express Forwarding operation on Ethernet interface 0:

```
Router(config)# ip cef distributed
Router(config)# interface e0
Router(config-if)# ip route-cache distributed
```

Configuring Fast Switching for Traffic That Is Received and Transmitted over the Same Interface

The following example shows how to enable fast switching and disable Cisco Express Forwarding switching:

```
Router(config)# interface ethernet 0/0/0
Router(config-if)# ip route-cache same-interface
```

The following example shows that fast switching on the same interface is enabled for interface fastethernet 0/0/0:

```
Router# show ip interface fastEthernet 0/0/0

FastEthernet0/0/0 is up, line protocol is up
  Internet address is 10.1.1.254/24
  Broadcast address is 255.255.255.224
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  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 Distributed switching is disabled
  IP Feature Fast switching turbo vector
  IP Null turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast
  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
  IP multicast multilayer switching is disabled
```

The following example shows the configuration information for FastEthernet interface 0/0/0:

```
Router# show running-config
.
.
!
interface FastEthernet0/0/0
 ip address 10.1.1.254 255.255.255.0
 ip route-cache same-interface
 no ip route-cache cef
 no ip route-cache distributed
!
```

Enabling NetFlow Accounting

The following example shows how to enable NetFlow switching:

```
Router(config)# interface ethernet 0/0/0
Router(config-if)# ip route-cache flow
```

The following example shows that NetFlow accounting is enabled for FastEthernet interface 0/0/0:

```
Router# show ip interface fastEthernet 0/0/0

FastEthernet0/0/0 is up, line protocol is up
  Internet address is 10.1.1.254/24
  Broadcast address is 255.255.255.224
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  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 enabled
  IP Distributed switching is disabled
  IP Flow switching turbo vector
  IP Null turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, Flow
  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
  IP multicast multilayer switching is disabled
```

Configuring Distributed Switching

The following example shows how to enable distributed switching:

```
Router(config)# ip cef distributed
Router(config)# interface ethernet 0/0/0
Router(config-if)# ip route-cache distributed
```

The following example shows that distributed Cisco Express Forwarding switching is for FastEthernet interface 0/0/0:

```
Router# show cef interface fastEthernet 0/0/0

FastEthernet0/0/0 is up (if_number 3)
  Corresponding hwidb fast_if_number 3
  Corresponding hwidb firstsw->if_number 3
  Internet address is 10.1.1.254/24
  ICMP redirects are always sent
  Per packet load-sharing is disabled
  IP unicast RPF check is disabled
  Inbound access list is not set
  Outbound access list is not set
  IP policy routing is disabled
  Hardware idb is FastEthernet0/0/0
  Fast switching type 1, interface type 18
  IP Distributed CEF switching enabled
  IP Feature Fast switching turbo vector
  IP Feature CEF switching turbo vector
  Input fast flags 0x0, Output fast flags 0x0
  ifindex 1(1)
  Slot 0 Slot unit 0 VC -1
  Transmit limit accumulator 0x48001A02 (0x48001A02)
  IP MTU 1500
```

Configuring Fast Switching for PBR

The following example shows how to configure a simple policy-based routing scheme and to enable FSPBR:

```
Router(config)# access-list 1 permit 10.1.1.0 0.0.0.255
Router(config)# route-map mypbrtag permit 10
Router(config-route-map)# match ip address 1
Router(config-route-map)# set ip next-hop 10.1.1.195
```

```
Router(config-route-map)# exit
Router(config)# interface fastethernet 0/0/0
Router(config-if)# ip route-cache policy
Router(config-if)# ip policy route-map mypbrtag
```

The following example shows that FSPBR is enabled for FastEthernet interface 0/0/0:

```
Router# show ip interface fastEthernet 0/0/0

FastEthernet0/0/0 is up, line protocol is up
  Internet address is 10.1.1.254/24
  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
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  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 Distributed switching is enabled
  IP Feature Fast switching turbo vector
  IP Feature CEF switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, Distributed, Policy, 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 enabled, using route map my_pbr_tag
  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
  IP multicast multilayer switching is disabled
```

Related Commands

Command	Description
exit	Leaves aggregation cache mode.
ip cef	Enables Cisco Express Forwarding on the RP card.
ip cef distributed	Enables distributed Cisco Express Forwarding operation.
ip flow ingress	Configures NetFlow on a subinterface.
set default interface	Configures a default interface for PBR.
set interface	Configures a specified interface for PBR.
set ip default next-hop	Configures a default IP next hop for PBR.
show cef interface	Displays detailed Cisco Express Forwarding information for interfaces.
show ip interface	Displays the usability status of interfaces configured for IP.
show mpoa client	Displays the routing table cache used to fast switch IP traffic.

ip router isis

To configure an Intermediate System-to-Intermediate System (IS-IS) routing process for IP on an interface and to attach an area designator to the routing process, use the **ip router isis** command in interface configuration mode. To disable IS-IS for IP, use the **no** form of the command.

ip router isis *area-tag*

no ip router isis *area-tag*

Syntax Description

area-tag	Meaningful name for a routing process. If it is not specified, a null tag is assumed and the process is referenced with a null tag. This name must be unique among all IP or Connectionless Network Service (CLNS) router processes for a given router. Required for multiarea IS-IS configuration. Optional for conventional IS-IS configuration. **Note** Each area in a multiarea configuration should have a nonnull area tag to facilitate identification of the area.

Defaults

No routing processes are specified.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
10.0	This command was introduced.
12.0(5)T	Multiarea functionality was added, changing the way the *tag* argument (now *area-tag*) is used.
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	Support for IPv6 was added.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
15.1(2)S	This command was integrated into Cisco IOS Release 15.1(2)S.

Usage Guidelines

Before the IS-IS routing process is useful, a network entity title (NET) must be assigned with the **net** command and some interfaces must have IS-IS enabled.

If you have IS-IS running and at least one International Organization for Standardization Interior Gateway Routing Protocol (ISO-IGRP) process, the IS-IS process and the ISO-IGRP process cannot both be configured without an area tag. The null tag can be used by only one process. If you run

ISO-IGRP and IS-IS, a null tag can be used for IS-IS, but not for ISO-IGRP at the same time. However, each area in an IS-IS multiarea configuration should have a nonnull area tag to facilitate identification of the area.

You can configure only one process to perform Level 2 (interarea) routing. If Level 2 routing is configured on any process, all additional processes are automatically configured as Level 1. You can configure this process to perform intra-area (Level 1) routing at the same time. You can configure up to 29 additional processes as Level 1-only processes. Use the **is-type** command to remove Level 2 routing from a router instance. You can then use the **is-type** command to enable Level 2 routing on some other IS-IS router instance.

An interface cannot be part of more than one area, except in the case where the associated routing process is performing both Level 1 and Level 2 routing. On media such as WAN media where subinterfaces are supported, different subinterfaces could be configured for different areas.

Examples

The following example specifies IS-IS as an IP routing protocol for a process named Finance, and specifies that the Finance process will be routed on Ethernet interface 0 and serial interface 0:

```
router isis Finance
 net 49.0001.aaaa.aaaa.aaaa.00
interface Ethernet 0
 ip router isis Finance
interface serial 0
 ip router isis Finance
```

The following example shows an IS-IS configuration with two Level 1 areas and one Level 1-2 area:

```
ip routing

.
.
.

interface Tunnel529
 ip address 10.0.0.5 255.255.255.0
 ip router isis BB

interface Ethernet1
 ip address 10.1.1.5 255.255.255.0
 ip router isis A3253-01
!
interface Ethernet2
 ip address 10.2.2.5 255.255.255.0
 ip router isis A3253-02


.
.
.

! Defaults to "is-type level-1-2"
router isis BB
 net 49.2222.0000.0000.0005.00
!
router isis A3253-01
 net 49.0553.0001.0000.0000.0005.00
 is-type level-1
!
router isis A3253-02
 net 49.0553.0002.0000.0000.0005.00
 is-type level-1
```

Related Commands

Command	Description
is-type	Configures the routing level for an IS-IS routing process.
net	Configures an IS-IS NET for a CLNS routing process.
router isis	Enables the IS-IS routing protocol.

ip source-address (telephony-service)

To identify the IP address and port through which IP phones communicate with a Cisco Unified CME router, use the **ip source-address** command in telephony-service or group configuration mode. To disable the router from receiving messages from Cisco Unified IP phones, use the **no** form of this command.

ip source-address {*ipv4_address* | *ipv6_address*} [**port** *port*] [**secondary** {*ipv4 address* | *ipv6 address*} [**rehome** *seconds*]] [**any-match** | **strict-match**]

no ip source-address

Syntax Description

ipv4_address	IPv4 address of the router, typically one of the addresses of the Ethernet port of the router.
ipv6_address	In Cisco Unified CME 8.0 and later versions: IPv6 address of the router, typically one of the addresses of the Ethernet port of the router.
port *port*	(Optional) TCP/IP port number to use for Skinny Client Control Protocol (SCCP). Default is 2000. For IPv4 only: Range is from 2000 to 9999. **Note** For IPv6, do not configure the port number to change from the default value (2000).
secondary	(Optional) Second Cisco Unified CME router with which phones can register if the primary Cisco Unified CME router fails. **Note** For dual-stack (IPv4 and IPv6) mode: Only an IPv4 address can be configured for a secondary router.
rehome *seconds*	(Optional) Used only by Cisco Unified IP phones that have registered with a Cisco Unified Survivable Remote Site Telephony (SRST) router. This keyword defines a delay that is used by phones to verify the stability of their primary SCCP controller (Cisco Unified Communications Manager or Cisco Unified CME) before the phones reregister with it. This parameter is ignored by phones unless they are registered to a secondary Cisco Unified SRST router. The range is from 0 to 65535 seconds. The default is 120 seconds. The use of this parameter is a phone behavior and is subject to change, based on the phone type and phone firmware version.
strict-match	(Optional) Requires strict IP address checking for registration.

Command Default

The IP address for communicating with phones is not defined.

Command Modes

Telephony-service configuration (config-telephony)
Group configuration (conf-tele-group)

Command History

Cisco IOS Release	Cisco Product	Modification
12.1(5)YD	Cisco ITS 1.0	This command was introduced.
12.2(8)T	Cisco ITS 2.0	This command was integrated into Cisco IOS Release 12.2(8)T.
12.4(4)XC	Cisco Unified CME 4.0	The **secondary** *ip-address* and **rehome** *seconds* keyword-argument pairs were added.
12.4(9)T	Cisco Unified CME 4.0	The **secondary** *ip-address* and **rehome** *seconds* keyword-argument pairs were added.
12.4(22)T	Cisco Unified CME 7.0(1)	This command was added to VRF group mode.
15.0(1)XA	Cisco Unified CME 8.0	This command was modified. Support for IPv6 was added and the *ipv4-address* and ipv6-*address* arguments replaced the generic *ip-address* argument.
15.1(1)T	Cisco Unified CME 8.0	This command was integrated into Cisco IOS Release 15.1(1)T.

Usage Guidelines

This command enables a router to receive messages from Cisco Unified IP phones through the specified IP address and port.

The Cisco Unified CME router cannot communicate with Cisco Unified CME phones if the IP address of the port to which they are attached is not configured. In Cisco Unified CME 8.0 and later versions, the Cisco Unified CME router can receive messages from IPv6-enabled or IPv4-enabled IP phones or from phones in dual-stack (both IPv6 and IPv4) mode.

- In Cisco Unified CME 8.0 and later versions: If the IP phones connected to Cisco Unified CME were configured for dual-stack mode by using **dual-stack** keyword with the **protocol mode** command, configure this command with the IPv6 address.
- In Cisco Unified CME 8.0 and later versions: If the IP phones to be connected to the port to be configured are IPv4-enabled only *or* IPv6-enabled only, configure this command with the corresponding IPv4 or IPv6 address.

For IPv6: Do not configure the **port** *port* keyword argument combination in this command to change the value from the default (2000). If you change the port number, IPv6 CEF packet switching engine will not be able to handle the IPv6 SCCP phones and various packet handling problems may occur when more than a dozen (approximately) calls in IPv6 are going on.

Use the **strict-match** keyword to instruct the router to reject IP phone registration attempts if the IP server address used by the phone does not match the source address.

Prior to Cisco IOS Telephony Services (Cisco ITS) V2.1, this command helped the router to autogenerate the SEPDEFAULT.cnf file, which was stored in the flash memory of the router. The SEPDEFAULT.cnf file contains the IP address of one of the Ethernet ports of the router to which the phone should register.

In ITS V2.1 and in Cisco CME 3.0 and later versions, the configuration files were moved to system:/its/. The file named Flash:SEPDEFAULT.cnf that was used with previous Cisco ITS versions is obsolete, but is retained as system:/its/SEPDEFAULT.cnf to support upgrades from older phone firmware.

For systems using Cisco ITS V2.1 or later versions, the IP phones receive their initial configuration information and phone firmware from the TFTP server associated with the router. In most cases, the phones obtain the IP address of their TFTP server using the **option 150** command and Dynamic Host Configuration Protocol (DHCP). For Cisco ITS or Cisco CME operation, the TFTP server address obtained by the Cisco Unified IP phones should point to the router IP address. The Cisco IP phones

attempt to transfer a configuration file called XmlDefault.cnf.xml. This file is automatically generated by the router through the **ip source-address** command and is placed in router memory. The XmlDefault.cnf.xml file contains the IP address that the phones use to register for service, using the SCCP. This IP address should correspond to a valid Cisco CME router IP address (and may be the same as the router TFTP server address).

Similarly, when an analog telephone adapter (ATA) such as the ATA-186 is attached to the Cisco Unified CME router, the ATA receives very basic configuration information and firmware from the TFTP server XmlDefault.cnf.xml file. The XmlDefault.cnf.xml file is automatically generated by the Cisco Unified CME router with the **ip source-address** command and is placed in the router's flash memory.

By specifying a second Cisco Unified CME router in the **ip source-address** command, you improve the failover time for phones.

Examples

The following example sets the IP source address and port:

```
Router(config)# telephony-service
Router(config-telephony)# ip source-address 10.6.21.4 port 2000 strict-match
```

The following example establishes the router at 10.5.2.78 as a secondary router:

```
Router(config)# telephony-service
Router(config-telephony)# ip source-address 10.0.0.1 port 2000 secondary 10.5.2.78
```

Cisco Unified CME 8.0 and later versions

The following example shows how to configure this command with an IPv6 address. Do not change the port number from the default value (2000) when you configure an IPv6 address.

```
Router(config)# telephony-service
Router(config-telephony)# protocol mode ipv6
Router(config-telephony)# ip source-address 2001:10:10:10::3
```

The following example shows how to configure an IP address for dual-stack mode. When the IP phones are configured for dual-stack mode, the IP address of the router port to which the IP phones are connected must be an IPv6 address. For dual-stack mode, the address of the secondary router must be an IPv4 address.

```
Router(config)# telephony-service
Router(config-telephony)# protocol mode dual-stack
Router(config-telephony)# ip source address 2001:10:10:10::3 secondary 10.5.2.78
Router(config-telephony)#
```

Related Commands

Command	Description
option	Configures DHCP server options.
protocol mode	Configures a preferred IP-address mode for SCCP IP phones in Cisco Unified CME.

ip unnumbered

To enable IP processing on an interface without assigning an explicit IP address to the interface, use the **ip unnumbered** command in interface configuration mode or subinterface configuration mode. To disable the IP processing on the interface, use the **no** form of this command.

ip unnumbered *type number*

no ip unnumbered *type number*

Syntax Description

type	Interface on which the router has assigned an IP address. The interface cannot be unnumbered interface. 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

IP processing on the unnumbered interface is disabled.

Command Modes

Interface configuration (config-if)
Subinterface configuration (config-subif)

Command History

Release	Modification
10.0	This command was introduced.
12.3(4)T	This command was modified to configure IP unnumbered support on Ethernet VLAN subinterfaces and subinterface ranges.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE. This command became available on the Supervisor Engine 720.
12.2(18)SXF	This command was modified to support Ethernet physical interfaces and switched virtual interfaces (SVIs).
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.
Cisco IOS XE Release 2.5	This command was implemented on Cisco ASR 1000 series routers.

Usage Guidelines

When an unnumbered interface generates a packet (for example, for a routing update), it uses the address of the specified interface as the source address of the IP packet. It also uses the address of the specified interface in determining which routing processes are sending updates over the unnumbered interface. Restrictions are as follows:

- This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 32.

- Serial interfaces using High-Level Data Link Control (HDLC), PPP, Link Access Procedure Balanced (LAPB), Frame Relay encapsulations, and Serial Line Internet Protocol (SLIP), and tunnel interfaces can be unnumbered. It is not possible to use this interface configuration command with X.25 or Switched Multimegabit Data Service (SMDS) interfaces.
- You cannot use the **ping** EXEC command to determine whether the interface is up because the interface has no address. Simple Network Management Protocol (SNMP) can be used to remotely monitor interface status.
- It is not possible to netboot a Cisco IOS image over a serial interface that is assigned an IP address with the **ip unnumbered** command.
- You cannot support IP security options on an unnumbered interface.

The interface you specify by the *type* and *'number* arguments must be enabled (listed as "up" in the **show interfaces** command display).

If you are configuring Intermediate System-to-Intermediate System (IS-IS) across a serial line, you should configure the serial interfaces as unnumbered. This configuration allows you to comply with RFC 1195, which states that IP addresses are not required on each interface.

Note Using an unnumbered serial line between different major networks (or *majornets*) requires special care. If at each end of the link there are different majornets assigned to the interfaces you specified as unnumbered, any routing protocol running across the serial line must not advertise subnet information.

Examples

In the following example, the first serial interface is given the address of Ethernet 0:

```
interface ethernet 0
 ip address 10.108.6.6 255.255.255.0
!
interface serial 0
 ip unnumbered ethernet 0
```

In the following example, Ethernet VLAN subinterface 3/0.2 is configured as an IP unnumbered subinterface:

```
interface ethernet 3/0.2
 encapsulation dot1q 200
 ip unnumbered ethernet 3/1
```

In the following example, Fast Ethernet subinterfaces in the range from 5/1.1 to 5/1.4 are configured as IP unnumbered subinterfaces:

```
interface range fastethernet5/1.1 - fastethernet5/1.4
 ip unnumbered ethernet 3/1
```

ipv6 access-class

To filter incoming and outgoing connections to and from the router based on an IPv6 access list, use the **ipv6 access-class** command in line configuration mode. To disable the filtering of incoming and outgoing connections to the router, use the **no** form of this command.

ipv6 access-class *ipv6-access-list-name* {**in** | **out**}

no ipv6 access-class

Syntax Description

ipv6-access-list-name	Name of an IPv6 access list. Names cannot contain a space or quotation mark, or begin with a numeric.
in	Filters incoming IPv6 connections.
out	Filters outgoing IPv6 connections.

Command Default

The filtering of incoming and outgoing connections to and from the router is not enabled.

Command Modes

Line configuration

Command History

Release	Modification
12.2(2)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 Release 12.2(14)S.
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.
12.2(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 introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The **ipv6 access-class** command is similar to the **access-class** command, except that it is IPv6-specific.

Identical restrictions should be set on all the virtual terminal lines because a user can connect to any of them.

The incoming connection source address is used to match against the access list source prefix. The router address on the received interface is used to match against the access list destination prefix.

IPv6 access control list (ACL) matches are made using TCP; an ACL permit match using IPv6 or TCP is required to allow access to a router.

Examples

The following example filters incoming connections on virtual terminal lines 0 to 4 of the router based on the IPv6 access list named cisco:

```
ipv6 access-list cisco
 permit ipv6 host 2001:0DB8:0:4::2/128 any

line vty 0 4
 ipv6 access-class cisco in
```

Related Commands

Command	Description
ipv6 access-list	Defines an IPv6 access list and sets deny or permit conditions for the defined access list.
ipv6 traffic-filter	Filters incoming or outgoing IPv6 traffic on an interface.
show ipv6 access-list	Displays the contents of all current IPv6 access lists.

ipv6 access-list

To define an IPv6 access list and to place the router in IPv6 access list configuration mode, use the **ipv6 access-list** command in global configuration mode. To remove the access list, use the **no** form of this command.

ipv6 access-list *access-list-name*

no ipv6 access-list *access-list-name*

Syntax Description

access-list-name	Name of the IPv6 access list. Names cannot contain a space or quotation mark, or begin with a numeric.

Command Default

No IPv6 access list is defined.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)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.
12.0(23)S	Support for IPv6 address configuration mode and extended access list functionality (the filtering of traffic based on IPv6 option headers and optional, upper-layer protocol type information) was added. Additionally, the following keywords and arguments were moved from global configuration mode to IPv6 access list configuration mode: **permit**, **deny,** *source-ipv6-prefix*/*prefix-length*, **any**, *destination-ipv6-prefix*/*prefix-length*, **priority**. See the "Usage Guidelines" section for more details.
12.2(13)T	Support for IPv6 address configuration mode and extended access list functionality (the filtering of traffic based on IPv6 option headers and optional, upper-layer protocol type information) was added. Additionally, the following keywords and arguments were moved from global configuration mode to IPv6 access list configuration mode: **permit**, **deny,** *source-ipv6-prefix*/*prefix-length*, **any**, *destination-ipv6-prefix*/*prefix-length*, **priority**. See the "Usage Guidelines" section for more details.
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.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2(33)SXH	Duplicate remark statements can no longer be configured from the IPv6 access control list.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 series routers.

Usage Guidelines

The **ipv6 access-list** command is similar to the **ip access-list** command, except that it is IPv6-specific.

In Cisco IOS Release 12.2(2)T or later releases, 12.0(21)ST, and 12.0(22)S, standard IPv6 access control list (ACL) functionality is used for basic traffic filtering functions—traffic filtering is based on source and destination addresses, inbound and outbound to a specific interface, and with an implicit deny statement at the end of each access list (functionality similar to standard ACLs in IPv4). IPv6 ACLs are defined and their deny and permit conditions are set by using the **ipv6 access-list** command with the **deny** and **permit** keywords in global configuration mode.

In Cisco IOS Release 12.0(23)S or later releases, the standard IPv6 ACL functionality is extended to support—in addition to traffic filtering based on source and destination addresses—filtering of traffic based on IPv6 option headers and optional, upper-layer protocol type information for finer granularity of control (functionality similar to extended ACLs in IPv4). IPv6 ACLs are defined by using the **ipv6 access-list** command in global configuration mode and their permit and deny conditions are set by using the **deny** and **permit** commands in IPv6 access list configuration mode. Configuring the **ipv6 access-list** command places the router in IPv6 access list configuration mode—the router prompt changes to Router(config-ipv6-acl)#. From IPv6 access list configuration mode, permit and deny conditions can be set for the defined IPv6 ACL.

Note IPv6 ACLs are defined by a unique name (IPv6 does not support numbered ACLs). An IPv4 ACL and an IPv6 ACL cannot share the same name.

In Cisco IOS Release 12.0(23)S or later releases, and 12.2(11)S or later releases, for backward compatibility, the **ipv6 access-list** command with the **deny** and **permit** keywords in global configuration mode is still supported; however, an IPv6 ACL defined with deny and permit conditions in global configuration mode is translated to IPv6 access list configuration mode.

Refer to the **deny** (IPv6) and **permit** (IPv6) commands for more information on filtering IPv6 traffic based on IPv6 option headers and optional, upper-layer protocol type information. See the “Examples” section for an example of a translated IPv6 ACL configuration.

Note In Cisco IOS Release 12.0(23)S or later releases, every IPv6 ACL has implicit **permit icmp any any nd-na**, **permit icmp any any nd-ns**, and **deny ipv6 any any** statements as its last match conditions. (The former two match conditions allow for ICMPv6 neighbor discovery.) An IPv6 ACL must contain at least one entry for the implicit **deny ipv6 any any** statement to take effect.

The IPv6 neighbor discovery process makes use of the IPv6 network layer service; therefore, by default, IPv6 ACLs implicitly allow IPv6 neighbor discovery packets to be sent and received on an interface. In IPv4, the Address Resolution Protocol (ARP), which is equivalent to the IPv6 neighbor discovery process, makes use of a separate data link layer protocol; therefore, by default, IPv4 ACLs implicitly allow ARP packets to be sent and received on an interface.

Note IPv6 prefix lists, not access lists, should be used for filtering routing protocol prefixes.

Use the **ipv6 traffic-filter** interface configuration command with the *access-list-name* argument to apply an IPv6 ACL to an IPv6 interface. Use the **ipv6 access-class** line configuration command with the *access-list-name* argument to apply an IPv6 ACL to incoming and outgoing IPv6 virtual terminal connections to and from the router.

Note An IPv6 ACL applied to an interface with the **ipv6 traffic-filter** command filters traffic that is forwarded, not originated, by the router.

Note When using this command to modify an ACL that is already associated with a bootstrap router (BSR) candidate rendezvous point (RP) (see the **ipv6 pim bsr candidate rp** command) or a static RP (see the **ipv6 pim rp-address** command), any added address ranges that overlap the PIM SSM group address range (FF3x::/96) are ignored. A warning message is generated and the overlapping address ranges are added to the ACL, but they have no effect on the operation of the configured BSR candidate RP or static RP commands.

In Cisco IOS Release 12.2(33)SXH and subsequent Cisco IOS SX releases, duplicate remark statements can no longer be configured from the IPv6 access control list. Because each remark statement is a separate entity, each one is required to be unique.

Examples

The following example is from a router running Cisco IOS Release 12.0(23)S or later releases. The example configures the IPv6 ACL list named list1 and places the router in IPv6 access list configuration mode.

```
Router(config)# ipv6 access-list list1
Router(config-ipv6-acl)#
```

The following example is from a router running Cisco IOS Release 12.2(2)T or later releases, 12.0(21)ST, or 12.0(22)S. The example configures the IPv6 ACL named list2 and applies the ACL to outbound traffic on Ethernet interface 0. Specifically, the first ACL entry keeps all packets from the network FEC0:0:0:2::/64 (packets that have the site-local prefix FEC0:0:0:2 as the first 64 bits of their source IPv6 address) from exiting out of Ethernet interface 0. The second entry in the ACL permits all other traffic to exit out of Ethernet interface 0. The second entry is necessary because an implicit deny all condition is at the end of each IPv6 ACL.

```
Router(config)# ipv6 access-list list2 deny FEC0:0:0:2::/64 any
Router(config)# ipv6 access-list list2 permit any any

Router(config)# interface ethernet 0
Router(config-if)# ipv6 traffic-filter list2 out
```

If the same configuration was entered on a router running Cisco IOS Release 12.0(23)S or later releases, the configuration would be translated into IPv6 access list configuration mode as follows:

```
ipv6 access-list list2
  deny FEC0:0:0:2::/64 any
  permit ipv6 any any

interface ethernet 0
 ipv6 traffic-filter list2 out
```

Note IPv6 is automatically configured as the protocol type in **permit any any** and **deny any any** statements that are translated from global configuration mode to IPv6 access list configuration mode.

Note IPv6 ACLs defined on a router running Cisco IOS Release 12.2(2)T or later releases, 12.0(21)ST, or 12.0(22)S that rely on the implicit deny condition or specify a **deny any any** statement to filter traffic should contain **permit** statements for link-local and multicast addresses to avoid the filtering of protocol packets (for example, packets associated with the neighbor discovery protocol). Additionally, IPv6 ACLs that use **deny** statements to filter traffic should use a **permit any any** statement as the last statement in the list.

Note An IPv6 router will not forward to another network an IPv6 packet that has a link-local address as either its source or destination address (and the source interface for the packet is different from the destination interface for the packet).

Related Commands

Command	Description
deny (IPv6)	Sets deny conditions for an IPv6 access list.
ipv6 access-class	Filters incoming and outgoing connections to and from the router based on an IPv6 access list.
ipv6 pim bsr candidate rp	Configures the candidate RP to send PIM RP advertisements to the BSR.
ipv6 pim rp-address	Configure the address of a PIM RP for a particular group range.
ipv6 traffic-filter	Filters incoming or outgoing IPv6 traffic on an interface.
permit (IPv6)	Sets permit conditions for an IPv6 access list.
show ipv6 access-list	Displays the contents of all current IPv6 access lists.

ipv6 access-list log-update threshold

To specify the number of updates that are logged for IPv6 access lists, use the **ipv6 access-list log-update threshold** command in global configuration mode. To return the number of logged updates to the default setting, use the **no** form of this command.

ipv6 access-list log-update threshold *value*

no ipv6 access-list log-update threshold

Syntax Description

value	Specifies the number of updates that are logged for every IPv6 access list configured on the router. The acceptable range is from 0 to 2147483647.

Command Default

The default is 2147483647 updates.

Command Modes

Global configuration

Command History

Release	Modification
12.0(23)S	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(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.

Usage Guidelines

The **ipv6 access-list log-update threshold** command is similar to the **ip access-list log-update threshold** command, except that it is IPv6-specific.

IPv6 ACL updates are logged at five minute intervals, following the first logged update. Configuring a lower number of updates (a number lower than the default) is useful when more frequent update logging is desired.

Examples

The following example configures a log threshold of ten updates for every IPv6 access list configured on the router.

```
ipv6 access-list log-update threshold 10
```

Related Commands

Command	Description
ipv6 access-list	Defines an IPv6 access list and enters IPv6 access list configuration mode.
show ipv6 access-list	Displays the contents of all current IPv6 access lists.

ipv6 address

To configure an IPv6 address based on an IPv6 general prefix and enable IPv6 processing on an interface, use the **ipv6 address** command in interface configuration mode. To remove the address from the interface, use the **no** form of this command.

ipv6 address {*ipv6-address*/*prefix-length* | *prefix-name sub-bits*/*prefix-length*}

no ipv6 address {*ipv6-address*/*prefix-length* | *prefix-name sub-bits*/*prefix-length*}

Syntax Description

ipv6-address	The IPv6 address to be used.
/*prefix-length*	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
prefix-name	A general prefix, which specifies the leading bits of the network to be configured on the interface.
sub-bits	The subprefix bits and host bits of the address to be concatenated with the prefixes provided by the general prefix specified with the *prefix-name* argument. The *sub-bits* argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

Command Default

No IPv6 addresses are defined for any interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
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.
12.2(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 introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The **ipv6 address** command allows multiple IPv6 addresses to be configured on an interface in various different ways, with varying options. The most common way is to specify the IPv6 address with the prefix length.

Addresses may also be defined using the general prefix mechanism, which separates the aggregated IPv6 prefix bits from the subprefix and host bits. In this case, the leading bits of the address are defined in a general prefix, which is globally configured or learned (for example, through use of Dynamic Host Configuration Protocol-Prefix Delegation (DHCP-PD)), and then applied using the *prefix-name* argument. The subprefix bits and host bits are defined using the *sub-bits* argument.

Using the **no ipv6 address autoconfig** command without arguments removes all IPv6 addresses from an interface.

IPv6 link-local addresses must be configured and IPv6 processing must be enabled on an interface by using the **ipv6 address link-local** command.

Examples

The following example shows how to enable IPv6 processing on the interface and configure an address based on the general prefix called my-prefix and the directly specified bits:

```
Router(config-if) ipv6 address my-prefix 0:0:0:7272::72/64
```

Assuming the general prefix named my-prefix has the value of 2001:DB8:2222::/48, then the interface would be configured with the global address 2001:DB8:2222:7272::72/64.

Related Commands

Command	Description
ipv6 address anycast	Configures an IPv6 anycast address and enables IPv6 processing on an interface.
ipv6 address eui-64	Configures an IPv6 address and enables IPv6 processing on an interface using an EUI-64 interface ID in the low-order 64 bits of the address.
ipv6 address link-local	Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface.
ipv6 unnumbered	Enables IPv6 processing on an interface without assigning an explicit IPv6 address to the interface.
no ipv6 address autoconfig	Removes all IPv6 addresses from an interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 address anycast

To configure an IPv6 anycast address and enable IPv6 processing on an interface, use the **ipv6 address anycast** command in interface configuration mode. To remove the address from the interface, use the **no** form of this command.

ipv6 address *ipv6-prefix*/*prefix-length* **anycast**

no ipv6 address [*ipv6-prefix*/*prefix-length* **anycast**]

Syntax Description

ipv6-prefix	The IPv6 network assigned to the interface. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/*prefix-length*	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

Command Default

No IPv6 addresses are defined for any interface.

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.
12.2(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.
12.2(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

Using the **no ipv6 address** command without arguments removes all manually configured IPv6 addresses from an interface.

Examples

The following example shows how to enable IPv6 processing on the interface, assign the prefix 2001:0DB8:1:1::/64 to the interface, and configure the IPv6 anycast address 2001:0DB8:1:1:FFFF:FFFF:FFFF:FFFE:

```
ipv6 address 2001:0DB8:1:1:FFFF:FFFF:FFFF:FFFE/64 anycast
```

Related Commands

Command	Description
ipv6 address eui-64	Configures an IPv6 address and enables IPv6 processing on an interface using an EUI-64 interface ID in the low-order 64 bits of the address.
ipv6 address link-local	Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface.
ipv6 unnumbered	Enables IPv6 processing on an interface without assigning an explicit IPv6 address to the interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 address autoconfig

To enable automatic configuration of IPv6 addresses using stateless autoconfiguration on an interface and enable IPv6 processing on the interface, use the **ipv6 address autoconfig** command in interface configuration mode. To remove the address from the interface, use the **no** form of this command.

ipv6 address autoconfig [**default**]

no ipv6 address autoconfig

Syntax Description

default	(Optional) If a default router is selected on this interface, the **default** keyword causes a default route to be installed using that default router. The **default** keyword can be specified only on one interface.

Command Default

No IPv6 address is defined for the interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 2.5	This command was updated. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

The **ipv6 address autoconfig** command causes the device to perform IPv6 stateless address auto-configuration to discover prefixes on the link and then to add the EUI-64 based addresses to the interface. Addresses are configured depending on the prefixes received in Router Advertisement messages.

Using the **no ipv6 address autoconfig** command without arguments removes all IPv6 addresses from an interface.

Examples

The following example assigns the IPv6 address automatically:

```
Router(config)# interface ethernet 0
Router(config-if)# ipv6 address autoconfig
```

Related Commands

Command	Description
ipv6 address eui-64	Configures an IPv6 address and enables IPv6 processing on an interface using an EUI-64 interface ID in the low-order 64 bits of the address.
ipv6 address link-local	Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface.
ipv6 unnumbered	Enables IPv6 processing on an interface without assigning an explicit IPv6 address to the interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 address dhcp

To acquire an IPv6 address on an interface from the Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server, use the **ipv6 address dhcp** command in the interface configuration mode. To remove the address from the interface, use the **no** form of this command.

ipv6 address dhcp [**rapid-commit**]

no ipv6 address dhcp

Syntax Description

rapid-commit	(Optional) Allows the two-message exchange method for address assignment.

Command Default

No IPv6 addresses are acquired from the DHCPv6 server.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(24)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

The **ipv6 address dhcp** interface configuration command allows any interface to dynamically learn its IPv6 address by using DHCP.

The **rapid-commit** keyword enables the use of the two-message exchange for address allocation and other configuration. If it is enabled, the client includes the rapid-commit option in a solicit message.

Examples

The following example shows how to acquire an IPv6 address and enable the rapid-commit option:

```
Router(config)# interface fastethernet 0/0
Router(config-if)# ipv6 address dhcp rapid-commit
```

You can verify your settings by using the **show ipv6 dhcp interface** command in privileged EXEC mode.

Related Commands

Command	Description
show ipv6 dhcp interface	Displays DHCPv6 interface information.

ipv6 address dhcp client request

To configure an IPv6 client to request a vendor-specific option from a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server, use the **ipv6 address dhcp client request** command in interface configuration mode. To remove the request, use the **no** form of this command.

ipv6 address dhcp client request vendor

no ipv6 address dhcp client request vendor

Syntax Description

vendor	Requests the vendor-specific options.

Command Default

IPv6 clients are not configured to request an option from DHCP.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(24)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

Use the **ipv6 address dhcp client request vendor** command to request a vendor-specific option. When this command is enabled, the IPv6 client can request a vendor-specific option only when an IPv6 address is acquired from DHCP. If you enter the command after the interface has acquired an IPv6 address, the IPv6 client cannot request a vendor-specific option until the next time the client acquires an IPv6 address from DHCP.

Examples

The following example shows how to configure an interface to request vendor-specific options:

```
Router(config)# interface fastethernet 0/0
Router(config-if)# ipv6 address dhcp client request vendor
```

Related Commands

Command	Description
ipv6 address dhcp	Acquires an IPv6 address on an interface from the DHCPv6 server.

ipv6 address eui-64

To configure an IPv6 address for an interface and enables IPv6 processing on the interface using an EUI-64 interface ID in the low order 64 bits of the address, use the **ipv6 address eui-64** command in interface configuration mode. To remove the address from the interface, use the **no** form of this command.

ipv6 address *ipv6-prefix*/*prefix-length* **eui-64**

no ipv6 address [*ipv6-prefix*/*prefix-length* **eui-64**]

Syntax Description

ipv6-prefix	The IPv6 network assigned to the interface. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/*prefix-length*	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

Command Default

No IPv6 address is defined for the interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)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 Release 12.2(14)S.
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.
12.2(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 introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

If the value specified for the /*prefix-length* argument is greater than 64 bits, the prefix bits have precedence over the interface ID.

Using the **no ipv6 address** command without arguments removes all manually configured IPv6 addresses from an interface.

If the Cisco IOS software detects another host using one of its IPv6 addresses, it will display an error message on the console.

Examples

The following example assigns IPv6 address 2001:0DB8:0:1::/64 to Ethernet interface 0 and specifies an EUI-64 interface ID in the low order 64 bits of the address:

```
Router(config)# interface ethernet 0
Router(config-if)# ipv6 address 2001:0DB8:0:1::/64 eui-64
```

Related Commands

Command	Description
ipv6 address link-local	Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface.
ipv6 unnumbered	Enables IPv6 processing on an interface without assigning an explicit IPv6 address to the interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 address link-local

To configure an IPv6 link-local address for an interface and enable IPv6 processing on the interface, use the **ipv6 address link-local** command in interface configuration mode. To remove the address from the interface, use the **no** form of this command.

ipv6 address *ipv6-address*/*prefix-length* **link-local** [**cga**]

no ipv6 address [*ipv6-address*/*prefix-length* **link-local**]

Syntax Description

ipv6-address	The IPv6 address assigned to the interface. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/*prefix-length*	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
link-local	Specifies a link-local address. The *ipv6-address* specified with this command overrides the link-local address that is automatically generated for the interface.
cga	(Optional) Specifies the CGA interface identifier.

Command Default

No IPv6 address is defined for the interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)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 Release 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 introduced on Cisco ASR 1000 Series Routers.
12.4(24)T	The **cga** keyword was added

Usage Guidelines

Using the **no ipv6 address** command without arguments removes all manually configured IPv6 addresses from an interface.

If the Cisco IOS software detects another host using one of its IPv6 addresses, it will display an error message on the console.

The system automatically generates a link-local address for an interface when IPv6 processing is enabled on the interface, typically when an IPv6 address is configured on the interface. To manually specify a link-local address to be used by an interface, use the **ipv6 address link-local** command.

A double colon may be used as part of the *ipv6-address* argument when consecutive 16-bit values are denoted as zero. You can configure multiple IPv6 addresses per interfaces, but only one link-local address.

Examples

The following example assigns FE80::260:3EFF:FE11:6770 as the link-local address for Ethernet interface 0:

```
interface ethernet 0
 ipv6 address FE80::260:3EFF:FE11:6770 link-local
```

Related Commands

Command	Description
ipv6 address eui-64	Configures an IPv6 address and enables IPv6 processing on an interface using an EUI-64 interface ID in the low-order 64 bits of the address.
ipv6 unnumbered	Enables IPv6 processing on an interface without assigning an explicit IPv6 address to the interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 atm-vc

To configure a mapping between a virtual circuit (VC) and the IPv6 address of a system at the far end of that circuit, use the **ipv6 atm-vc** command in map-list configuration mode. To remove the mapping, use the **no** form of this command.

ipv6 *ipv6-address* **atm-vc** *vcd* [**broadcast**]

no ipv6 *ipv6-address* **atm-vc** *vcd* [**broadcast**]

Syntax Description

ipv6-address	The IPv6 address of a system at the far end of the specified virtual circuit. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
vcd	The virtual circuit descriptor for the virtual circuit mapped to the specified IPv6 address.
broadcast	(Optional) Specifies that this map entry is used when sending IPv6 multicast packets to the interface (for example, network routing protocol updates).

Command Default

No default behavior or values.

Command Modes

Map-list configuration

Command History

Release	Modification
12.2(2)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 Release 12.2(14)S.
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.
12.2(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

ATM permanent virtual circuits (PVCs) can be configured in the following modes:

- Nonbroadcast multiaccess (NBMA) mode—A neighbor is mapped to a PVC. ATM point-to-multipoint PVCs are configured using static maps. The **ipv6 atm-vc** command utilizes static maps.
- Point-to point-mode—Each PVC is given a subinterface and is configured as a standard point-to-point link.

Note We recommend configuring ATM PVCs in point-to-point mode.

Examples

The following example maps neighbor 2001:0DB8::5 to ATM point-to-multipoint PVC 1, virtual path identifier (VPI) 3, and virtual channel identifier (VCI) 5:

```
Router(config)# interface atm 1/0
Router(config-if)# atm pvc 1 3 5 aal5snap
Router(config-if)# map-group cisco

Router(config)# map-list cisco
Router(config-map-list)# ipv6 2001:0DB8::5 atm-vc 1
```

Related Commands

Command	Description
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 authentication key-chain eigrp

To enable authentication of Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 packets, use the **ipv6 authentication key-chain eigrp** command in interface configuration mode. To disable authentication of EIGRP for IPv6 packets, use the **no** form of this command.

ipv6 authentication key-chain eigrp *as-number key-chain*

no ipv6 authentication key-chain eigrp *as-number key-chain*

Syntax Description

as-number	Autonomous system number.
key-chain	Name of the authentication key chain.

Command Default

No authentication is provided for EIGRP for IPv6 packets.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(6)T	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.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

EIGRP for IPv6 route authentication provides Message Digest 5 (MD5) authentication of routing updates from the EIGRP for IPv6 routing protocol. The MD5 keyed digest in each EIGRP for IPv6 packet prevents the introduction of unauthorized or false routing messages from unapproved sources.

Each key has its own key identifier, which is stored locally. The combination of the key identifier and the interface associated with the message uniquely identifies the authentication algorithm and MD5 authentication key in use.

You can configure multiple keys with lifetimes. Only one authentication packet is sent, regardless of how many valid keys exist. The software examines the key numbers in order from lowest to highest, and uses the first valid key it encounters.

Examples

The following example enables authentication for EIGRP for IPv6 for AS 1, using a key chain named chain1:

```
Router(config-if)# ipv6 authentication key-chain eigrp 1 chain1
```

Related Commands

Command	Description
accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.
ipv6 authentication mode eigrp	Specifies the type of authentication used in EIGRP for IPv6 packets.
key	Identifies an authentication key on a key chain.
key chain	Enables authentication of routing protocols.
key-string (authentication)	Specifies the authentication string for a key.
send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.

ipv6 authentication mode eigrp

To specify the type of authentication used in Enhanced Interior Gateway Routing Protocol (EIGRP) packets for IPv6, use the **ipv6 authentication mode eigrp** command in interface configuration mode. To disable the type of authentication, use the **no** form of this command.

ipv6 authentication mode eigrp *as-number* **md5**

no ipv6 authentication mode eigrp *as-number* **md5**

Syntax Description

as-number	Autonomous system number.
md5	Specifies keyed message digest 5 (MD5) authentication.

Command Default

No authentication is provided for EIGRP for IPv6 packets.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(6)T	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.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

Use the **ipv6 authentication mode eigrp** command to configure authentication to prevent unapproved sources from introducing unauthorized or false routing messages. When authentication is configured, an MD5 keyed digest is added to each EIGRP for IPv6 packet in the specified autonomous system.

Examples

The following example configures the interface to use MD5 authentication in EIGRP for IPv6 packets in autonomous system 1:

```
Router(config-if)# ipv6 authentication mode eigrp 1 md5
```

Related Commands

Command	Description
accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.
ipv6 authentication key-chain eigrp	Enables authentication of EIGRP packets for IPv6.
key	Identifies an authentication key on a key chain.
key chain	Enables authentication of routing protocols.

Command	Description
key-string (authentication)	Specifies the authentication string for a key.
send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.

ipv6 bandwidth-percent eigrp

To configure the percentage of bandwidth that may be used by Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 on an interface, use the **ipv6 bandwidth-percent eigrp** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ipv6 bandwidth-percent eigrp *as-number percent*

no ipv6 bandwidth-percent eigrp *as-number percent*

Syntax Description

as-number	Autonomous system number.
percent	Percentage of bandwidth that EIGRP for IPv6 may use.

Command Default

Percentage of bandwidth used is 50 percent.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(6)T	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.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

EIGRP for IPv6 uses as much as 50 percent of the bandwidth of a link, as defined by the **bandwidth** command. The **ipv6 bandwidth-percent eigrp** command may be used if some other fraction of the bandwidth is desired.

Note that values greater than 100 percent may be configured. The configuration option may be useful if the bandwidth is set artificially low for other reasons.

Examples

The following example allows EIGRP for IPv6 to use up to 75 percent (42 kbps) of a 56-kbps serial link in autonomous system 1:

```
interface serial 0
 bandwidth 56
 ipv6 bandwidth-percent eigrp 1 75
```

Related Commands

Command	Description
bandwidth (interface)	Sets a bandwidth value for an interface.

ipv6 cef

To enable Cisco Express Forwarding for IPv6, use the **ipv6 cef** command in global configuration mode. To disable Cisco Express Forwarding for IPv6, use the **no** form of this command.

ipv6 cef

no ipv6 cef

Syntax Description

This command has no arguments or keywords.

Command Default

Cisco Express Forwarding for IPv6 is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(22)S	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(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.
12.2(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 implemented on Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

The **ipv6 cef** command is similar to the **ip cef** command, except that it is IPv6-specific.

The **ipv6 cef** command is not available on the Cisco 12000 series Internet routers because this distributed platform operates only in distributed Cisco Express Forwarding for IPv6 mode.

Note The **ipv6 cef** command is not supported in interface configuration mode.

Note Some distributed architecture platforms, such as the Cisco 7500 series routers, support both Cisco Express Forwarding for IPv6 and distributed Cisco Express Forwarding for IPv6. When Cisco Express Forwarding for IPv6 is configured on distributed platforms, Cisco Express Forwarding switching is performed by the Route Processor (RP).

Note You must enable Cisco Express Forwarding for IPv4 by using the **ip cef** global configuration command before enabling Cisco Express Forwarding for IPv6 by using the **ipv6 cef** global configuration command.

Cisco Express Forwarding for IPv6 is advanced Layer 3 IP switching technology that functions the same and offer the same benefits as Cisco Express Forwarding for IPv4. Cisco Express Forwarding for IPv6 optimizes network performance and scalability for networks with dynamic, topologically dispersed traffic patterns, such as those associated with web-based applications and interactive sessions.

Examples

The following example enables standard Cisco Express Forwarding for IPv4 operation and then standard Cisco Express Forwarding for IPv6 operation globally on the router.

```
ip cef
ipv6 cef
```

Related Commands

Command	Description
ip route-cache	Controls the use of high-speed switching caches for IP routing.
ipv6 cef accounting	Enables Cisco Express Forwarding for IPv6 and distributed Cisco Express Forwarding for IPv6 network accounting.
ipv6 cef distributed	Enables distributed Cisco Express Forwarding for IPv6.
show cef	Displays which packets the line cards dropped or displays which packets were not express-forwarded.
show ipv6 cef	Displays entries in the IPv6 FIB.

ipv6 cef accounting

To enable Cisco Express Forwarding for IPv6 and distributed Cisco Express Forwarding for IPv6 network accounting, use the **ipv6 cef accounting** command in global configuration mode or interface configuration mode. To disable Cisco Express Forwarding for IPv6 network accounting, use the **no** form of this command.

ipv6 cef accounting *accounting-types*

no ipv6 cef accounting *accounting-types*

Specific Cisco Express Forwarding Accounting Information Through Interface Configuration Mode

ipv6 cef accounting non-recursive {**external** | **internal**}

no ipv6 cef accounting non-recursive {**external** | **internal**}

Syntax Description

accounting-types	The *accounting-types* argument must be replaced with at least one of the following keywords. Optionally, you can follow this keyword by any or all of the other keywords, but you can use each keyword only once. • **load-balance-hash**—Enables load balancing hash bucket counters. • **non-recursive**—Enables accounting through nonrecursive prefixes. • **per-prefix**—Enables express forwarding of the collection of the number of packets and bytes to a destination (or prefix). • **prefix-length**—Enables accounting through prefix length.
non-recursive	Enables accounting through nonrecursive prefixes. This keyword is optional when used in global configuration mode after another keyword is entered. See the *accounting-types* argument.
external	Counts input traffic in the nonrecursive external bin.
internal	Counts input traffic in the nonrecursive internal bin.

Command Default

Cisco Express Forwarding for IPv6 network accounting is disabled by default.

Command Modes

Global configuration (config)
Interface configuration (config-if)

Command History

Release	Modification
12.0(22)S	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.

Release	Modification
12.2(25)S	The **non-recursive** and **load-balance-hash** keywords 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.
12.2(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 introduced on Cisco ASR 1000 Series Routers.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The **ipv6 cef accounting** command is similar to the **ip cef accounting** command, except that it is IPv6-specific.

Configuring Cisco Express Forwarding for IPv6 network accounting enables you to collect statistics on Cisco Express Forwarding for IPv6 traffic patterns in your network.

When you enable network accounting for Cisco Express Forwarding for IPv6 by using the **ipv6 cef accounting** command in global configuration mode, accounting information is collected at the Route Processor (RP) when Cisco Express Forwarding for IPv6 mode is enabled and at the line cards when distributed Cisco Express Forwarding for IPv6 mode is enabled. You can then display the collected accounting information using the **show ipv6 cef** EXEC command.

For prefixes with directly connected next hops, the **non-recursive** keyword enables express forwarding of the collection of packets and bytes through a prefix. This keyword is optional when this command is used in global configuration mode after you enter another keyword on the **ipv6 cef accounting** command.

This command in interface configuration mode must be used in conjunction with the global configuration command. The interface configuration command allows a user to specify two different bins (internal or external) for the accumulation of statistics. The internal bin is used by default. The statistics are displayed through the **show ipv6 cef detail** command.

Per-destination load balancing uses a series of 16 hash buckets into which the set of available paths are distributed. A hash function operating on certain properties of the packet is applied to select a bucket that contains a path to use. The source and destination IP addresses are the properties used to select the bucket for per-destination load balancing. Use the **load-balance-hash** keyword with the **ipv6 cef accounting** command to enable per-hash-bucket counters. Enter the **show ipv6 cef** *prefix* **internal** command to display the per-hash-bucket counters.

Examples

The following example enables the collection of Cisco Express Forwarding for IPv6 accounting information for prefixes with directly connected next hops:

```
Router(config)# ipv6 cef accounting non-recursive
```

Related Commands

Command	Description
ip cef accounting	Enable Cisco Express Forwarding network accounting (for IPv4).
show cef	Displays information about packets forwarded by Cisco Express Forwarding.
show ipv6 cef	Displays entries in the IPv6 FIB.

ipv6 cef distributed

To enable distributed Cisco Express Forwarding for IPv6, use the **ipv6 cef distributed** command in global configuration mode. To disable Cisco Express Forwarding for IPv6, use the **no** form of this command.

ipv6 cef distributed

no ipv6 cef distributed

Syntax Description

This command has no arguments or keywords.

Command Default

Distributed Cisco Express Forwarding for IPv6 is disabled on the Cisco 7500 series routers and enabled on the Cisco 12000 series Internet routers.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(22)S	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(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.
12.2(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 implemented on Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

The **ipv6 cef distributed** command is similar to the **ip cef distributed** command, except that it is IPv6-specific.

Enabling distributed Cisco Express Forwarding for IPv6 globally on the router by using the **ipv6 cef distributed** in global configuration mode distributes the Cisco Express Forwarding processing of IPv6 packets from the Route Processor (RP) to the line cards of distributed architecture platforms.

Note The **ipv6 cef distributed** command is not supported on the Cisco 12000 series Internet routers because distributed Cisco Express Forwarding for IPv6 is enabled by default on this platform.

Note To forward distributed Cisco Express Forwarding for IPv6 traffic on the router, configure the forwarding of IPv6 unicast datagrams globally on your router by using the **ipv6 unicast-routing** global configuration command, and configure an IPv6 address and IPv6 processing on an interface by using the **ipv6 address** interface configuration command.

Note You must enable distributed Cisco Express Forwarding for IPv4 by using the **ip cef distributed** global configuration command before enabling distributed Cisco Express Forwarding for IPv6 by using the **ipv6 cef distributed** global configuration command.

Cisco Express Forwarding is advanced Layer 3 IP switching technology. Cisco Express Forwarding optimizes network performance and scalability for networks with dynamic, topologically dispersed traffic patterns, such as those associated with web-based applications and interactive sessions.

Examples

The following example enables distributed Cisco Express Forwarding for IPv6 operation:

```
ipv6 cef distributed
```

Related Commands

Command	Description
ip route-cache	Controls the use of high-speed switching caches for IP routing.
show ipv6 cef	Displays entries in the IPv6 FIB.

ipv6 cef load-sharing algorithm

To select a Cisco Express Forwarding load-balancing algorithm for IPv6, use the **ipv6 cef load-sharing algorithm** command in global configuration mode. To return to the default universal load-balancing algorithm, use the **no** form of this command.

ipv6 cef load-sharing algorithm {**original** | **universal** [*id*] | **include-ports** {**source** [*id*] | [**destination**] [*id*] | **source** [*id*] **destination** [*id*]}}

no ipv6 cef load-sharing algorithm

Syntax Description

original	Sets the load-balancing algorithm to the original algorithm based on a source and destination hash.
universal	Sets the load-balancing algorithm to the universal algorithm that uses a source and destination and an ID hash.
id	(Optional) Fixed identifier in hexadecimal format.
include-ports source	Sets the load-balancing algorithm to the include-ports algorithm that uses a Layer 4 source port.
include-ports destination	Sets the load-balancing algorithm to the include-ports algorithm that uses a Layer 4 destination port.
include-ports source destination	Sets the load balancing algorithm to the include-ports algorithm that uses Layer 4 source and destination ports.

Command Default

The universal load-balancing algorithm is selected. If you do not configure the fixed identifier for a load-balancing algorithm, the router automatically generates a unique ID.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(25)S	This command was introduced.
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.
12.2(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	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The **ipv6 cef load-sharing algorithm** command is similar to the **ip cef load-sharing algorithm** command, except that it is IPv6-specific.

When the Cisco Express Forwarding for IPv6 load-balancing algorithm is set to universal mode, each router on the network can make a different load-sharing decision for each source-destination address pair.

The include-ports algorithm allows you to use the Layer 4 source and destination ports as part of the load-balancing decision. This method benefits traffic streams running over equal-cost paths that are not load-shared because the majority of the traffic is between peer addresses that use different port numbers, such as Real-Time Protocol (RTP) streams.

Examples

The following example shows how to enable the Cisco Express Forwarding load-balancing algorithm for IPv6 for Layer-4 source and destination ports:

```
Router(config)# ipv6 cef load-sharing algorithm include-ports source destination
```

The router automatically generates fixed IDs for the algorithm.

Related Commands

Command	Description
debug ipv6 cef hash	Displays debug messages for Cisco Express Forwarding for IPv6 and distributed Cisco Express Forwarding for IPv6 load-sharing hash algorithm events.
ip cef load-sharing algorithm	Selects a Cisco Express Forwarding load-balancing algorithm (for IPv4).

ipv6 cef optimize neighbor resolution

To configure address resolution optimization from Cisco Express Forwarding for IPv6 for directly connected neighbors, use the **ipv6 cef optimize neighbor resolution** command in global configuration mode. To disable address resolution optimization from Cisco Express Forwarding for IPv6 for directly connected neighbors, use the **no** form of this command.

ipv6 cef optimize neighbor resolution

no ipv6 cef optimize neighbor resolution

Syntax Description

This command has no arguments or keywords.

Command Default

If this command is not configured, Cisco Express Forwarding for IPv6 does not optimize the address resolution of directly connected neighbors.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(25)S	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.
12.2(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

The **ipv6 cef optimize neighbor resolution** command is very similar to the **ip cef optimize neighbor resolution** command, except that it is IPv6-specific.

Use this command to trigger Layer 2 address resolution of neighbors directly from Cisco Express Forwarding for IPv6.

Examples

The following example shows how to optimize address resolution from Cisco Express Forwarding for IPv6 for directly connected neighbors:

```
Router(config)# ipv6 cef optimize neighbor resolution
```

Related Commands

Command	Description
ip cef optimize neighbor resolution	Configures address resolution optimization from Cisco Express Forwarding for IPv4 for directly connected neighbors.

ipv6 cga modifier rsakeypair

To generate an IPv6 cryptographically generated address (CGA) modifier for a specified Rivest, Shamir, and Adelman (RSA) key pair, use the **ipv6 cga modifier rsakeypair** command in global configuration mode. To disable this function, use the **no** form of this command.

ipv6 cga modifier rsakeypair *key-label* **sec-level** {**0** | **1**}

no ipv6 cga modifier rsakeypair

Syntax Description

key-label	The name to be used for RSA key pair
sec-level {**0** | **1**}	Specifies the security level, which can be either 0 or 1. The most secure level is 1.

Command Default

No CGA exists for an RSA key.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

Use this command to generate the CGA modifier for a specified RSA key pair, which enables the key to be used by Secure Neighbor Discovery (SeND).

Once the RSA key is generated, the modifier must be generated as well, using the **ipv6 cga modifier rsakeypair** command.

A CGA has a security parameter that determines its strength against brute-force attacks. The security level can be either 0 or 1.

Examples

The following example enables the specified key to be used by SeND (that is, generates the modifier):

```
Router(config)# ipv6 cga modifier rsakeypair SEND sec-level 1
```

Related Commands

Command	Description
crypto key generate rsa	Generates RSA key pairs.
ipv6 cga modifier rsakeypair	Generates the CGA modifier for a specified RSA key.
ipv6 cga modifier rsakeypair (interface)	Binds a SeND key to a specified interface.
ipv6 cga rsakeypair	Specifies which RSA key should be used on an interface.

ipv6 cga rsakeypair

To bind a Secure Neighbor Discovery (SeND) key to a specified interface, use the **ipv6 cga rsakeypair** command in interface configuration mode. To disable this function, use the **no** form of this command.

ipv6 cga rsakeypair *key-label*

no ipv6 cga rsakeypair

Syntax Description		
	key-label	The name to be used for the Rivest, Shamir, and Adelman (RSA) key pair.

Command Default

A SeND key is not bound to an interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

The SeND key is used to generate an IPv6 modifier for a specified Rivest, Shamir and Adelman (RSA) key pair. A SeND key must be bound to the interface prior to its being used in the **ipv6 address** command. Use the **ipv6 cga rsakeypair** command to bind a SeND key to a specified interface.

You can then use the **ipv6 address** command to add the Cryptographic Addresses (CGA).

Examples

The following example binds a SeND key to Ethernet interface 0/0:

```
Router(config)# interface Ethernet0/0
Router(config-if)# ip address 10.0.1.1 255.255.255.0
Router(config-if)# ipv6 cga rsakeypair SEND
```

Related Commands

Command	Description
ipv6 address	Configures an IPv6 address based on an IPv6 general prefix and enables IPv6 processing on an interface.
crypto key generate rsa	Generates RSA key pairs.
ipv6 cga modifier rsakeypair (global configuration)	Generates the CGA modifier for a specified RSA key.
ipv6 cga modifier rsakeypair (interface configuration)	Binds a SeND key to a specified interface.
ipv6 cga rsakeypair	Specifies which RSA key should be used on an interface.

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.

ipv6 dhcp binding track ppp

To configure Dynamic Host Configuration Protocol (DHCP) for IPv6 to release any bindings associated with a PPP connection when that connection closes, use the **ipv6 dhcp binding track ppp** command in global configuration mode. To return to the default behavior, use the **no** form of this command.

ipv6 dhcp binding track ppp

no ipv6 dhcp binding track ppp

Syntax Description

This command has no arguments or keywords.

Command Default

When a PPP connection closes, the DHCP bindings associated with that connection are not released.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.5	This command was introduced.

Usage Guidelines

The **ipv6 dhcp binding track ppp** command configures DHCP for IPv6 to automatically release any bindings associated with a PPP connection when that connection is closed. The bindings are released automatically to accommodate subsequent new registrations by providing sufficient resource.

A binding table entry on the DHCP for IPv6 server is automatically:

- Created whenever a prefix is delegated to a client from the configuration pool.
- Updated when the client renews, rebinds, or confirms the prefix delegation.
- Deleted when the client releases all the prefixes in the binding voluntarily, all prefixes' valid lifetimes have expired, or an administrator clears the binding.

Examples

The following example shows how to release the prefix bindings associated with the PPP:

```
Router(config)# ipv6 dhcp binding track ppp
```

ipv6 dhcp client information refresh minimum

To configure the minimum acceptable Dynamic Host Configuration Protocol (DHCP) for IPv6 client information refresh time on a specified interface, use the **ipv6 dhcp client information refresh minimum** command in interface configuration mode. To remove the configured refresh time, use the **no** form of this command.

ipv6 dhcp client information refresh minimum *seconds*

no ipv6 dhcp client information refresh minimum *seconds*

Syntax Description

seconds	The refresh time, in seconds. The minimum value that can be used is 600 seconds.

Command Default

The default is 86,400 seconds (24 hours).

Command Modes

Interface configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

The **ipv6 dhcp client information refresh minimum** command specifies the minimum acceptable information refresh time. If the server sends an information refresh time option of less than the configured minimum refresh time, the configured minimum refresh time will be used instead.

This command may be configured in several situations:

- In unstable environments where unexpected changes are likely to occur.
- For planned changes, including renumbering. An administrator can gradually decrease the time as the planned event nears.
- Limit the amount of time before new services or servers are available to the client, such as the addition of a new Simple Network Time Protocol (SNTP) server or a change of address of a Domain Name System (DNS) server.

Examples

The following example configures an upper limit of 2 hours:

```
ipv6 dhcp client information refresh minimum 7200
```

ipv6 dhcp client pd

To enable the Dynamic Host Configuration Protocol (DHCP) for IPv6 client process and enable request for prefix delegation through a specified interface, use the **ipv6 dhcp client pd** command in interface configuration mode. To disable requests for prefix delegation, use the **no** form of this command.

ipv6 dhcp client pd {*prefix-name* | **hint** *ipv6-prefix*} [**rapid-commit**]

no ipv6 dhcp client pd

Syntax Description

prefix-name	IPv6 general prefix name.
hint	An IPv6 prefix sent as a hint.
ipv6-prefix	IPv6 general prefix.
rapid-commit	(Optional) Allow two-message exchange method for prefix delegation.

Command Default

Prefix delegation is disabled on an interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

Enabling the **ipv6 dhcp client pd** command starts the DHCP for IPv6 client process if this process is not yet running.

The **ipv6 dhcp client pd** command enables request for prefix delegation through the interface on which this command is configured. When prefix delegation is enabled and a prefix is successfully acquired, the prefix is stored in the IPv6 general prefix pool with an internal name defined by the *ipv6-prefix* argument. Other commands and applications (such as the **ipv6 address** command) can then refer to the prefixes in the general prefix pool.

The **hint** keyword with the *ipv6-prefix* argument enables the configuration of an IPv6 prefix that will be included in DHCP for IPv6 solicit and request messages sent by the DHCP for IPv6 client on the interface as a hint to prefix-delegating routers. Multiple prefixes can be configured by issuing the **ipv6 dhcp client pd hint** *ipv6-prefix* command multiple times. The new prefixes will not overwrite old ones.

The **rapid-commit** keyword enables the use of the two-message exchange for prefix delegation and other configuration. If it is enabled, the client will include the rapid commit option in a solicit message.

The DHCP for IPv6 client, server, and relay functions are mutually exclusive on an interface. When one of these functions is already enabled and a user tries to configure a different function on the same interface, one of the following messages is displayed: “Interface is in DHCP client mode,” “Interface is in DHCP server mode,” or “Interface is in DHCP relay mode.”

Examples

The following example enables prefix delegation:

```
Router(config-if)# ipv6 dhcp client pd dhcp-prefix
```

The following example configures a hint for prefix-delegating routers:

```
Router(config-if)# ipv6 dhcp client pd hint 2001:0DB8:1/48
```

Related Commands

Command	Description
clear ipv6 dhcp client	Restarts the DHCP for IPv6 client on an interface.
show ipv6 dhcp interface	Displays DHCP for IPv6 interface information.

ipv6 dhcp database

To configure a Dynamic Host Configuration Protocol (DHCP) for IPv6 binding database agent, use the **ipv6 dhcp database** command in global configuration mode. To delete the database agent, use the **no** form of this command.

ipv6 dhcp database *agent* [**write-delay** *seconds*] [**timeout** *seconds*]

no ipv6 dhcp database *agent*

Syntax Description

agent	A flash, local bootflash, compact flash, NVRAM, FTP, TFTP, or Remote Copy Protocol (RCP) uniform resource locator.
write-delay *seconds*	(Optional) How often (in seconds) DHCP for IPv6 sends database updates. The default is 300 seconds. The minimum write delay is 60 seconds.
timeout *seconds*	(Optional) How long, in seconds, the router waits for a database transfer.

Command Default

Write-delay default is 300 seconds.
Timeout default is 300 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

The **ipv6 dhcp database** command specifies DHCP for IPv6 binding database agent parameters. The user may configure multiple database agents.

A binding table entry is automatically created whenever a prefix is delegated to a client from the configuration pool, updated when the client renews, rebinds, or confirms the prefix delegation, and deleted when the client releases all the prefixes in the binding voluntarily, all prefixes' valid lifetimes have expired, or administrators enable the **clear ipv6 dhcp binding** command. These bindings are maintained in RAM and can be saved to permanent storage using the *agent* argument so that the information about configuration such as prefixes assigned to clients is not lost after a system reload or power down. The bindings are stored as text records for easy maintenance.

Each permanent storage to which the binding database is saved is called the database agent. A database agent can be a remote host such as an FTP server or a local file system such as NVRAM.

The **write-delay** keyword specifies how often, in seconds, that DHCP sends database updates. By default, DHCP for IPv6 server waits 300 seconds before sending any database changes.

The **timeout** keyword specifies how long, in seconds, the router waits for a database transfer. Infinity is defined as 0 seconds, and transfers that exceed the timeout period are aborted. By default, the DHCP for IPv6 server waits 300 seconds before aborting a database transfer. When the system is going to reload, there is no transfer timeout so that the binding table can be stored completely.

Examples

The following example specifies DHCP for IPv6 binding database agent parameters and stores binding entries in TFTP:

```
ipv6 dhcp database tftp://10.0.0.1/dhcp-binding
```

The following example specifies DHCP for IPv6 binding database agent parameters and stores binding entries in bootflash:

```
ipv6 dhcp database bootflash
```

Related Commands

Command	Description
clear ipv6 dhcp binding	Deletes automatic client bindings from the DHCP for IPv6 server binding table
show ipv6 dhcp database	Displays DHCP for IPv6 binding database agent information.

ipv6 dhcp debug redundancy

To display debugging output for IPv6 DHCP high availability (HA) processing, use the **ipv6 dhcp debug redundancy** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

ipv6 dhcp debug redundancy

no ipv6 dhcp debug redundancy

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.

Usage Guidelines

Use the **ipv6 dhcp debug redundancy** command to display stateful switchover (SSO) state transitions and errors.

Examples

The following example enables IPv6 DHCP redundancy debugging:

```
Router# ipv6 dhcp debug redundancy
```

ipv6 dhcp framed password

To assign a framed prefix when using a RADIUS server, use the **ipv6 dhcp framed password** command in interface configuration mode. To remove the framed prefix, use the **no** form of this command.

ipv6 dhcp framed password *password*

no ipv6 dhcp framed password

Syntax Description

password	Password to be used with the RADIUS server.

Command Default

No framed prefix is assigned.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 2.5	This command was introduced.

Usage Guidelines

The **ipv6 dhcp framed password** command enables a user to request a framed prefix of a RADIUS server. When a PPPoE client requests a prefix from a network using the framed-prefix system, the RADIUS server should assign an address. However, the RADIUS server is configured to receive a password. Because the client does not send a password, the RADIUS server does not send a framed prefix.

Note Ordinarily, the **ipv6 dhcp framed password** command will not need to be used because a client will have been authenticated as part of PPP session establishment.

Examples

The following example shows how to configure a password to be used with the RADIUS server:

```
Router(config-if)# ipv6 dhcp framed password password1
```

ipv6 dhcp ping packets

To specify the number of packets a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server sends to a pool address as part of a ping operation, use the **ipv6 dhcp ping packets** command in global configuration mode. To prevent the server from pinging pool addresses, use the **no** form of this command.

ipv6 dhcp ping packets *number*

ipv6 dhcp ping packets

Syntax Description

number	The number of ping packets sent before the address is assigned to a requesting client. The valid range is from 0 to 10.

Command Default

No ping packets are sent before the address is assigned to a requesting client.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(24)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

The DHCPv6 server pings a pool address before assigning the address to a requesting client. If the ping is unanswered, the server assumes, with a high probability, that the address is not in use and assigns the address to the requesting client.

Setting the *number* argument to 0 turns off the DHCPv6 server ping operation

Examples

The following example specifies four ping attempts by the DHCPv6 server before further ping attempts stop:

```
Router(config)# ipv6 dhcp ping packets 4
```

Related Commands

Command	Description
clear ipv6 dhcp conflict	Clears an address conflict from the DHCPv6 server database.
show ipv6 dhcp conflict	Displays address conflicts found by a DHCPv6 server, or reported through a DECLINE message from a client.

ipv6 dhcp pool

To configure a Dynamic Host Configuration Protocol (DHCP) for IPv6 server configuration information pool and enter DHCP for IPv6 pool configuration mode, use the **ipv6 dhcp pool** command in global configuration mode. To delete a DHCP for IPv6 pool, use the **no** form of this command.

ipv6 dhcp pool *poolname*

no ipv6 dhcp pool *poolname*

Syntax Description

poolname	User-defined name for the local prefix pool. The pool name can be a symbolic string (such as "Engineering") or an integer (such as 0).

Command Default

DHCP for IPv6 pools are not configured.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

Use the **ipv6 dhcp pool** command to create a DHCP for IPv6 server configuration information pool. When the **ipv6 dhcp pool** command is enabled, the configuration mode changes to DHCP for IPv6 pool configuration mode. In this mode, the administrator can configure pool parameters, such as prefixes to be delegated and Domain Name System (DNS) servers, using the following commands:

- **address prefix** *IPv6-prefix* [**lifetime** {*valid-lifetime preferred-lifetime* | **infinite**}] sets an address prefix for address assignment. This address must be in hexadecimal, using 16-bit values between colons.
- **link-address** *IPv6-prefix* sets a link-address IPv6 prefix. When an address on the incoming interface or a link-address in the packet matches the specified IPv6-prefix, the server uses the configuration information pool. This address must be in hexadecimal, using 16-bit values between colons.
- **vendor-specific** *vendor-id* enables DHCPv6 vendor-specific configuration mode. Specify a vendor identification number. This number is the vendor IANA Private Enterprise Number. The range is 1 to 4294967295. The following configuration command is available:

– **suboption** *number* sets vendor-specific suboption number. The range is 1 to 65535. You can enter an IPv6 address, ASCII text, or a hex string as defined by the suboption parameters.

Note The **hex** value used under the **suboption** keyword allows users to enter only hex digits (0-f). Entering an invalid **hex** value does not delete the previous configuration.

Once the DHCP for IPv6 configuration information pool has been created, use the **ipv6 dhcp server** command to associate the pool with a server on an interface. If you do not configure an information pool, you need to use the **ipv6 dhcp server interface** configuration command to enable the DHCPv6 server function on an interface.

When you associate a DHCPv6 pool with an interface, only that pool services requests on the associated interface. The pool also services other interfaces. If you do not associate a DHCPv6 pool with an interface, it can service requests on any interface.

Not using any IPv6 address prefix means that the pool returns only configured options.

The **link-address** command allows matching a link-address without necessarily allocating an address. You can match the pool from multiple relays by using multiple link-address configuration commands inside a pool.

Since a longest match is performed on either the address pool information or the link information, you can configure one pool to allocate addresses and another pool on a subprefix that returns only configured options.

Examples

The following example specifies a DHCP for IPv6 configuration information pool named cisco1 and places the router in DHCP for IPv6 pool configuration mode:

```
Router(config)# ipv6 dhcp pool cisco1
Router(config-dhcpv6)#
```

The following example shows how to configure an IPv6 address prefix for the IPv6 configuration pool cisco1:

```
Router(config-dhcpv6)# address prefix 2001:1000::0/64
Router(config-dhcpv6)# end
```

The following example shows how to configure a pool named engineering with three link-address prefixes and an IPv6 address prefix:

```
Router# configure terminal
Router(config)# ipv6 dhcp pool engineering
Router(config-dhcpv6)# link-address 2001:1001::0/64
Router(config-dhcpv6)# link-address 2001:1002::0/64
Router(config-dhcpv6)# link-address 2001:2000::0/48
Router(config-dhcpv6)# address prefix 2001:1003::0/64
Router(config-dhcpv6)# end
```

The following example shows how to configure a pool named 350 with vendor-specific options:

```
Router# configure terminal
Router(config)# ipv6 dhcp pool 350
Router(config-dhcpv6)# vendor-specific 9
Router(config-dhcpv6-vs)# suboption 1 address 1000:235D::1
Router(config-dhcpv6-vs)# suboption 2 ascii "IP-Phone"
Router(config-dhcpv6-vs)# end
```

Related Commands

Command	Description
ipv6 dhcp server	Enables DHCP for IPv6 service on an interface.
show ipv6 dhcp pool	Displays DHCP for IPv6 configuration pool information.

ipv6 dhcp relay destination

To specify a destination address to which client messages are forwarded and to enable Dynamic Host Configuration Protocol (DHCP) for IPv6 relay service on the interface, use the **ipv6 dhcp relay destination** command in interface configuration mode. To remove a relay destination on the interface or to delete an output interface for a destination, use the **no** form of this command.

ipv6 dhcp relay destination *ipv6-address* [*interface-type interface-number* | **vrf** *vrf-name* | **global**]

no ipv6 dhcp relay destination *ipv6-address* [*interface-type interface-number* | **vrf** *vrf-name* | **global**]

Syntax Description

ipv6-address	Relay destination address. There are two types of relay destination address: • Link-scoped unicast or multicast IPv6 address. A user must specify an output interface for this kind of address. • Global or site-scoped unicast or multicast IPv6 address. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
interface-type interface-number	(Optional) Interface type and number that specifies the output interface for a destination. If this argument is configured, client messages are forwarded to the destination address through the link to which the output interface is connected.
vrf *vrf-name*	(Optional) Specifies the virtual routing and forwarding (VRF) associated with the relay destination IPv6 address.
global	(Optional) Specifies the relay destination when the relay destination is in the global address space and when the relay source is in a VRF.

Command Default

The relay function is disabled, and there is no relay destination on an interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(11)T	This command was introduced.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
15.1(2)S	This command was modified. The **vrf** *vrf-name* keyword and argument were added. The **global** keyword was added.
Cisco IOS XE Release 3.3S	This command was modified. The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

The **ipv6 dhcp relay destination** command specifies a destination address to which client messages are forwarded, and it enables DHCP for IPv6 relay service on the interface. When relay service is enabled on an interface, a DHCP for IPv6 message received on that interface will be forwarded to all configured relay destinations. The incoming DHCP for IPv6 message may have come from a client on that interface, or it may have been relayed by another relay agent.

The relay destination can be a unicast address of a server or another relay agent, or it may be a multicast address. There are two types of relay destination addresses:

- A link-scoped unicast or multicast IPv6 address, for which a user must specify an output interface
- A global or site-scoped unicast or multicast IPv6 address. A user can optionally specify an output interface for this kind of address.

If no output interface is configured for a destination, the output interface is determined by routing tables. In this case, it is recommended that a unicast or multicast routing protocol be running on the router.

Multiple destinations can be configured on one interface, and multiple output interfaces can be configured for one destination. When the relay agent relays messages to a multicast address, it sets the hop limit field in the IPv6 packet header to 32.

Unspecified, loopback, and node-local multicast addresses are not acceptable as the relay destination. If any one of them is configured, the message “Invalid destination address” is displayed.

Note that it is not necessary to enable the relay function on an interface for it to accept and forward an incoming relay reply message from servers. By default, the relay function is disabled, and there is no relay destination on an interface. The **no** form of the command removes a relay destination on an interface or deletes an output interface for a destination. If all relay destinations are removed, the relay service is disabled on the interface.

The DHCP for IPv6 client, server, and relay functions are mutually exclusive on an interface. When one of these functions is already enabled and a user tries to configure a different function on the same interface, one of the following messages is displayed: “Interface is in DHCP client mode,” “Interface is in DHCP server mode,” or “Interface is in DHCP relay mode.”

Examples

The following example sets the relay destination address on Ethernet interface 4/3:

```
ipv6 dhcp relay destination FE80::250:A2FF:FEBF:A056 ethernet 4/3
```

Related Commands

Command	Description
show ipv6 dhcp interface	Displays DHCP for IPv6 interface information.

ipv6 dhcp-relay option vpn

To enable the DHCP for IPv6 relay VRF-aware feature, use the **ipv6 dhcp-relay option vpn** command in global configuration mode. To disable the feature, use the **no** form of this command.

ipv6 dhcp-relay option vpn

no ipv6 dhcp-relay option vpn

Syntax Description

This command has no arguments or keywords.

Command Default

The DHCP for IPv6 relay VRF-aware feature is not enabled on the router.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(2)S	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

The **ipv6 dhcp-relay option vpn** command allows the DHCPv6 relay VRF-aware feature to be enabled globally on the router. If the **ipv6 dhcp relay option vpn** command is enabled on a specified interface, it overrides the global **ipv6 dhcp-relay option vpn** command.

Examples

The following example enables the DHCPv6 relay VRF-aware feature globally on the router:

```
Router(config)# ipv6 dhcp-relay option vpn
```

Related Commands

Command	Description
ipv6 dhcp relay option vpn	Enables the DHCPv6 relay VRF-aware feature on an interface.

ipv6 dhcp relay source-interface

To configure an interface to use as the source when relaying messages received on this interface, use the **ipv6 dhcp relay source-interface** command in interface configuration mode. To remove the interface from use as the source, use the **no** form of this command.

ipv6 dhcp relay source-interface *type number*

no ipv6 dhcp relay source-interface *type number*

Syntax Description

type number	Interface type and number that specifies output interface for a destination. If these arguments are configured, client messages are forwarded to the destination address through the link to which the output interface is connected.

Command Default

The address of the server-facing interface is used as the IPv6 relay source.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

If the configured interface is shut down, or if all of its IPv6 addresses are removed, the relay will revert to its standard behavior.

The interface configuration (using the **ipv6 dhcp relay source-interface** command in interface configuration mode) takes precedence over the global configuration if both have been configured.

Examples

The following example configures the Loopback 0 interface to be used as the relay source:

```
Router(config-if)# ipv6 dhcp relay source-interface loopback 0
```

Related Commands

Command	Description
ipv6 dhcp-relay source-interface	Enables DHCP for IPv6 service on an interface.

ipv6 dhcp-relay show bindings

To enable the DHCPv6 relay agent to list prefix delegation (PD) bindings, use the **ipv6 dhcp-relay show bindings** command in global configuration mode. To disable PD binding tracking, use the **no** form of this command.

ipv6 dhcp-relay show bindings

no ipv6 dhcp-relay show bindings

Syntax Description

This command has no arguments or keywords.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.

Usage Guidelines

The **ipv6 dhcp-relay show bindings** command lists the PD bindings that the relay agent is tracking. The command lists the bindings in the relay's radix tree, lists DHCPv6 relay routes, and prints each entry's prefix and length, client identity association identification (IAID), and lifetime.

Examples

The following example enables the DHCPv6 relay agent to list PD bindings:

```
Router# ipv6 dhcp-relay show bindings
```

ipv6 dhcp-relay source-interface

To configure an interface to use as the source when relaying messages, use the **ipv6 dhcp-relay source-interface** command in global configuration mode. To remove the interface from use as the source, use the **no** form of this command.

ipv6 dhcp-relay source-interface {*interface-type interface-number*}

no ipv6 dhcp-relay source-interface {*interface-type interface-number*}

Syntax Description

interface-type interface-number	(Optional) Interface type and number that specifies output interface for a destination. If this argument is configured, client messages are forwarded to the destination address through the link to which the output interface is connected.

Command Default

The address of the server-facing interface is used as the IPv6 relay source.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

If the configured interface is shut down, or if all of its IPv6 addresses are removed, the relay will revert to its standard behavior.

The interface configuration (using the **ipv6 dhcp relay source-interface** command in interface configuration mode) takes precedence over the global configuration if both have been configured.

Examples

The following example configures the Loopback 0 interface to be used as the relay source:

```
Router(config)# ipv6 dhcp-relay source-interface loopback 0
```

Related Commands

Command	Description
ipv6 dhcp relay source-interface	Enables DHCP for IPv6 service on an interface.

ipv6 dhcp-relay bulk-lease

To configure bulk lease query parameters, use the **ipv6 dhcp-relay bulk-lease** command in global configuration mode. To remove the bulk-lease query configuration, use the **no** form of this command.

ipv6 dhcp-relay bulk-lease {**data-timeout** *seconds* | **retry** *number*} [**disable**]

no ipv6 dhcp-relay bulk-lease [**disable**]

Syntax Description

data-timeout	(Optional) Bulk lease query data transfer timeout.
seconds	(Optional) The range is from 60 seconds to 600 seconds. The default is 300 seconds.
retry	(Optional) Sets the bulk lease query retries.
number	(Optional) The range is from 0 to 5. The default is 5.
disable	(Optional) Disables the DHCPv6 bulk lease query feature.

Command Default

Bulk lease query is enabled automatically when the DHCP for IPv6 (DHCPv6) relay agent feature is enabled.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

Use the **ipv6 dhcp-relay bulk-lease** command in global configuration mode to configure bulk lease query parameters, such as data transfer timeout and bulk-lease TCP connection retries.

The DHCPv6 bulk lease query feature is enabled automatically when the DHCPv6 relay agent is enabled. The DHCPv6 bulk lease query feature itself cannot be enabled using this command. To disable this feature, use the **ipv6 dhcp-relay bulk-lease** command with the **disable** keyword.

Examples

The following example shows how to set the bulk lease query data transfer timeout to 60 seconds:

```
Router(config)# ipv6 dhcp-relay bulk-lease data-timeout 60
```

Related Commands	Command	Description

ipv6 dhcp-relay option vpn

To enable the DHCP for IPv6 relay VRF-aware feature, use the **ipv6 dhcp-relay option vpn** command in global configuration mode. To disable the feature, use the **no** form of this command.

ipv6 dhcp-relay option vpn

no ipv6 dhcp-relay option vpn

Syntax Description

This command has no arguments or keywords.

Command Default

The DHCP for IPv6 relay VRF-aware feature is not enabled on the router.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(2)S	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

The **ipv6 dhcp-relay option vpn** command allows the DHCPv6 relay VRF-aware feature to be enabled globally on the router. If the **ipv6 dhcp relay option vpn** command is enabled on a specified interface, it overrides the global **ipv6 dhcp-relay option vpn** command.

Examples

The following example enables the DHCPv6 relay VRF-aware feature globally on the router:

```
Router(config)# ipv6 dhcp-relay option vpn
```

Related Commands

Command	Description
ipv6 dhcp relay option vpn	Enables the DHCPv6 relay VRF-aware feature on an interface.

ipv6 dhcp server

To enable Dynamic Host Configuration Protocol (DHCP) for IPv6 service on an interface, use the **ipv6 dhcp server** in interface configuration mode. To disable DHCP for IPv6 service on an interface, use the **no** form of this command.

ipv6 dhcp server [*poolname* | **automatic**] [**rapid-commit**] [**preference** *value*] [**allow-hint**]

no ipv6 dhcp server

Syntax Description

poolname	(Optional) User-defined name for the local prefix pool. The pool name can be a symbolic string (such as "Engineering") or an integer (such as 0).
automatic	(Optional) Enables the server to automatically determine which pool to use when allocating addresses for a client.
rapid-commit	(Optional) Allows the two-message exchange method for prefix delegation.
preference *value*	(Optional) Specifies the preference value carried in the preference option in the advertise message sent by the server. The range is from 0 to 255. The preference value defaults to 0.
allow-hint	(Optional) Specifies whether the server should consider delegating client suggested prefixes. By default, the server ignores client-hinted prefixes.

Command Default

DHCP for IPv6 service on an interface is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.4(24)T	The **automatic** keyword was added.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

The **ipv6 dhcp server** command enables DHCP for IPv6 service on a specified interface using the pool for prefix delegation and other configuration through that interface.

The **automatic** keyword enables the system to automatically determine which pool to use when allocating addresses for a client. When an IPv6 DHCP packet is received by the server, the server determines if it was received from a DHCP relay or if it was directly received from the client. If the packet was received from a relay, the server verifies the link-address field inside the packet associated

with the first relay that is closest to the client. The server matches this link address against all address prefix and link-address configurations in IPv6 DHCP pools to find the longest prefix match. The server selects the pool associated with the longest match.

If the packet was directly received from the client, the server performs this same matching, but it uses all the IPv6 addresses configured on the incoming interface when performing the match. Once again, the server selects the longest prefix match.

The **rapid-commit** keyword enables the use of the two-message exchange for prefix delegation and other configuration. If a client has included a rapid commit option in the solicit message and the **rapid-commit** keyword is enabled for the server, the server responds to the solicit message with a reply message.

If the **preference** keyword is configured with a value other than 0, the server adds a preference option to carry the preference value for the advertise messages. This action affects the selection of a server by the client. Any advertise message that does not include a preference option is considered to have a preference value of 0. If the client receives an advertise message that includes a preference option with a preference value of 255, the client immediately sends a request message to the server from which the advertise message was received.

If the **allow-hint** keyword is specified, the server will delegate a valid client-suggested prefix in the solicit and request messages. The prefix is valid if it is in the associated local prefix pool and it is not assigned to a device. If the **allow-hint** keyword is not specified, a hint is ignored and a prefix is delegated from the free list in the pool.

The DHCP for IPv6 client, server, and relay functions are mutually exclusive on an interface. When one of these functions is already enabled and a user tries to configure a different function on the same interface, one of the following messages is displayed:

```
Interface is in DHCP client mode
Interface is in DHCP server mode
Interface is in DHCP relay mode
```

Examples

The following example enables DHCP for IPv6 for the local prefix pool named server1:

```
Router(config-if)# ipv6 dhcp server server1
```

Related Commands

Command	Description
ipv6 dhcp pool	Configures a DHCP for IPv6 pool and enters DHCP for IPv6 pool configuration mode.
show ipv6 dhcp interface	Displays DHCP for IPv6 interface information.

ipv6 dhcp server vrf enable

To enable the DHCP for IPv6 server VRF-aware feature, use the **ipv6 dhcp server vrf enable** command in global configuration mode. To disable the feature, use the **no** form of this command.

ipv6 dhcp server vrf enable

no ipv6 dhcp server vrf enable

Syntax Description

This command has no arguments or keywords.

Command Default

The DHCPv6 server VRF-aware feature is not enabled on the router.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(2)S	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

The **ipv6 dhcp server option vpn** command allows the DHCPv6 server VRF-aware feature to be enabled globally on the router.

Examples

The following example enables the DHCPv6 server VRF-aware feature globally on the router:

```
Router(config)# ipv6 dhcp server option vpn
```

ipv6 eigrp

To enable Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 on a specified interface, use the **ipv6 eigrp** command in interface configuration mode. To disable EIGRP for IPv6, use the **no** form of this command.

ipv6 eigrp *as-number*

no ipv6 eigrp *as-number*

Syntax Description

as-number	Autonomous system number.

Command Default

EIGRP is not enabled on an IPv6 interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(6)T	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.

Usage Guidelines

Use the **ipv6 eigrp** command to enable EIGRP for IPv6 on a per-interface basis.

If an autonomous system is specified, EIGRP for IPv6 is enabled only for the specified autonomous system. Otherwise, EIGRP for IPv6 is specified throughout the interface.

Examples

The following example enables EIGRP for IPv6 for AS 1 on Ethernet interface 0:

```
Router(config)# interface ethernet0
Router(config-if)# ipv6 eigrp 1
```

Related Commands

Command	Description
ipv6 enable	Enables IPv6 processing on an interface that has not been configured with an explicit IPv6 address.
ipv6 router eigrp	Configures the EIGRP routing process in IPv6.

ipv6 enable

To enable IPv6 processing on an interface that has not been configured with an explicit IPv6 address, use the **ipv6 enable** command in interface configuration mode. To disable IPv6 processing on an interface that has not been configured with an explicit IPv6 address, use the **no** form of this command.

ipv6 enable

no ipv6 enable

Syntax Description

This command has no arguments or keywords.

Command Default

IPv6 is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)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 Release 12.2(14)S.
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.
12.2(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 **ipv6 enable** command automatically configures an IPv6 link-local unicast address on the interface while also enabling the interface for IPv6 processing. The **no ipv6 enable** command does not disable IPv6 processing on an interface that is configured with an explicit IPv6 address.

Examples

The following example enables IPv6 processing on Ethernet interface 0/0:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 enable
```

Related Commands

Command	Description
ipv6 address link-local	Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface.
ipv6 address eui-64	Configures an IPv6 address and enables IPv6 processing on an interface using an EUI-64 interface ID in the low-order 64 bits of the address.

Command	Description
ipv6 unnumbered	Enables IPv6 processing on an interface without assigning an explicit IPv6 address to the interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 flow

Note Effective with Cisco IOS Release 12.4(20)T, the **ipv6 flow** command is not available in Cisco software.

To enable or disable accounting for IPv6 packets arriving on an interface configured for 6PE, use the **ipv6 flow** command in interface configuration mode. To disable NetFlow on a subinterface, use the **no** form of this command.

ipv6 flow {**ingress** | **egress**}

no ipv6 flow {**ingress** | **egress**}

Syntax Description

egress	Enables IPv6 flow capture on outgoing packets.
ingress	Enables IPv6 flow capture for incoming packets.

Command Default

This command is not configured by default.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)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.
12.4(20)T	This command was removed.

Usage Guidelines

Note The NetFlow for IPv6 feature has been replaced by the IPv6 Flexible NetFlow feature. For information on this feature, see the *Cisco IOS Flexible NetFlow Features Roadmap*.

This command must be configured on all interfaces and subinterfaces where NetFlow capture should be enabled. Two commands for ingress and egress can be specified on the same interface. If a switched packet belongs to a flow that is captured at both the ingress and the egress point, it will be counted twice.

If you configure the **ipv6 flow ingress** command on a few selected subinterfaces and then configure the **ip flow ingress** command on the main interface, enabling the main interface will overwrite the **ip flow ingress** command and data collection will start from the main interface and from all the subinterfaces. In a scenario where you configure the **ipv6 flow ingress** command and then configure the **ip route-cache flow** command on the main interface, you can restore subinterface data collection by using the **no ip**

route-cache flow command. This configuration will disable data collection from the main interface and restore data collection to the subinterfaces you originally configured with the **ipv6 flow ingress** command.

Examples

The following example shows how to configure NetFlow on FastEthernet subinterface 6/3.0:

```
Router(config)# interface FastEthernet6/3.0
Router(config-subif)# ipv6 flow ingress
```

Related Commands

Command	Description
ip flow ingress	Enables NetFlow accounting for inbound (received) network traffic.
ipv6 flow mask	Records a specified number of bits of the source or destination address in the flow record.
show ipv6 flow cache	Displays a summary of the NetFlow cache statistics.
show ip cache flow	Displays a summary of NetFlow statistics.
show ip interface	Displays the usability status of interfaces configured for IP.

ipv6 flow mask

To specify the maximum number of source or destination address bits for IPv6 flow capture on a per-interface basis, use the **ipv6 flow mask** command in interface configuration mode. To disable the capture of address bits on an interface, use the **no** form of this command.

ipv6 flow mask {**source** | **destination**} **maximum** *max-address-length*

no ipv6 flow {**source** | **destination**}

Syntax Description

source	Specifies that the source address for the flow record is to be used.
destination	Specifies that the destination address for the flow record is to be used.
maximum	Specifies the maximum number of address bits to capture in the flow record. The value can be 1 to 128.

Command Default

This command is not configured by default.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)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

This command records only the indicated number of bits of the source or destination address in the flow record. As a consequence, flows are aggregated.

Examples

The following example shows a router configured to capture the first 64 bits of the source address for packets entering this interface:

```
Router(config)# interface FastEthernet6/3.0
Router(config-subif)# ipv6 flow mask source maximum 64
```

Related Commands

Command	Description
ipv6 flow mask option headers	Enables option headers for IPv6 capture on a per-interface basis.

ipv6 flow mask option-headers

To enable capture of specific IPv6 option headers on a per-interface basis, use the **ipv6 flow mask option-headers** command in subinterface configuration mode. To disable masking of IPv6 option headers on a subinterface, use the **no** form of this command.

ipv6 flow mask option-headers *value*

no ipv6 flow mask option-headers

Syntax Description

value	The configurable value for the option headers. Value is specified in hexadecimal in the range 0x0 through 0xFFFFFFFF.

Command Default

This command is not enabled.

Command Modes

Subinterface configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)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

The **ipv6 flow mask option-headers** command records option headers for all of the flows in the main cache. When this command is not enabled, flows are aggregated by whatever IPv6 option headers are found in the packet.

NetFlow Version 9 Options Template Format

The options template (and its corresponding options data record) is a new record type for NetFlow Version 9. Options are used to supply metadata about the NetFlow process itself. The format of the options template is detailed in Table 28 and field descriptions are given in Table 29.

Table 28 NetFlow Version 9 Options Template

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
FlowSet ID = 1															
Length															
Reserved Template ID > 255															
Option Scope Length															
Option Length															
Scope Field 1 Type															

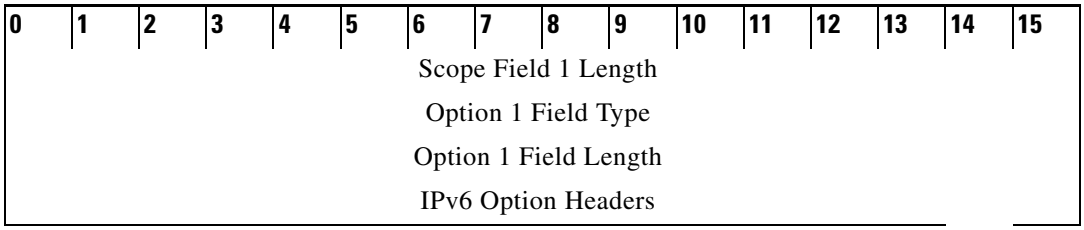

Table 29 NetFlow Version 9 Options Template Field Definitions

Field Name	Description
FlowSet ID = 1	The FlowSet ID is used to distinguish template records from data records. A template record always has a FlowSet ID of 1. A data record always has a nonzero FlowSet ID of greater than 255.
Length	This field gives the total length of this FlowSet. Because an individual template FlowSet may contain multiple template IDs, the length value should be used to determine the position of the next FlowSet record, which could be either a template or a data FlowSet. Length is expressed in type, length, value (TLV) format, meaning that the value includes the bytes used for the FlowSet ID and the length bytes themselves, and the combined lengths of all template records included in this FlowSet.
Reserved Template ID >255	As a router generates different template FlowSets to match the type of NetFlow data it will export, each template is given a unique ID. This uniqueness is local to the router that generated the template ID.
Option Scope Length	This field gives the length in bytes of any scope fields contained in this options template.
Options Length	This field gives the length (in bytes) of any Options field definitions contained in this options template.
Scope 1 Field Type	This field gives the relevant portion of the NetFlow process to which the options record refers. Values are as follows: • 0x0001 System • 0x0002 Interface • 0x0003 Line Card • 0x0004 NetFlow Cache • 0x0005 Template For example, sampled NetFlow can be implemented on a per-interface basis, so if the options record were reporting on how sampling is configured, the scope for the report would be 0x0002 (interface).
Scope 1 Field Length	This field gives the length (in bytes) of the Scope field, as it would appear in an options record.
Option 1 Field Type	This numeric value represents the type of the field that appears in the options record.

Option 1 Field Length	This number is the length (in bytes) of the field, as it would appear in an options record.
IPv6 Option Headers	This number exports encoded IPv6 option headers. Table 30 describes encoding for this field.

Table 30 provides information on encoding for the IPv6 Option Headers field.

Table 30 Encoded IPv6 Option Headers Fields

Bit 15	**Bit 14**	**Bit 13**	**Bit 12**	**Bit 11**	**Bit 10**	**Bit 9**	**Bit 8**
Reserved	Reserved	Reserved	Reserved	Reserved	Encrypted security payload (50)	Authentication header (51)	Payload compression header (108)
Bit 7	**Bit 6**	**Bit 5**	**Bit 4**	**Bit 3**	**Bit 2**	**Bit 1**	**Bit 0**
Destination option header (60)	Hop-by-hop option header (0)	Reserved	Cannot reach layer 4 header (for example, compressed, encrypted, not supported)	Fragmentation header (44)—first fragment	Routing header (43)	Fragmentation header (44)—not first fragment	Reserved

Examples

The following example shows a router configured to capture the option headers for packets passing through this interface:

```
Router(config)# interface FastEthernet6/3.0
Router(config-subif)# ipv6 flow mask option-headers 0x40
```

Related Commands

Command	Description
ipv6 flow mask	Records a specified number of bits of the source or destination address in the flow record.
show ipv6 cache flow	Displays a summary of IPv6 NetFlow statistics.

ipv6 flow-aggregation cache

Note Effective with Cisco IOS Release 12.4(20)T, the **ipv6 flow-aggregation cache** command is not available in Cisco software.

To configure the aggregation cache configuration scheme and place the router in NetFlow aggregation cache configuration mode, use the **ipv6 flow-aggregation cache** command in global configuration mode. To disable aggregation cache configuration mode, use the **no** form of this command.

ipv6 flow-aggregation cache {**as** | **bgp-nexthop** | **destination-prefix** | **prefix** | **protocol-port** | **source-prefix**}

no ipv6 flow-aggregation cache {**as** | **bgp-nexthop** | **destination-prefix** | **prefix** | **protocol-port** | **source-prefix**}

Syntax Description

as	Configures the autonomous system aggregation cache scheme.
bgp-nexthop	Configures the bgp-nexthop aggregation cache scheme to record the next Border Gateway Protocol (BGP) hop.
destination-prefix	Configures the destination-prefix aggregation cache scheme.
prefix	Configures the prefix aggregation cache scheme.
protocol-port	Configures the protocol-port aggregation cache scheme.
source-prefix	Configures the source-prefix aggregation cache scheme.

Command Default

This command is disabled by default. No aggregation cache information is collected.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)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.
12.4(20)T	This command was removed.

Usage Guidelines

You can enable only one aggregation cache configuration scheme per command line.

Note The NetFlow for IPv6 feature has been replaced by the IPv6 Flexible NetFlow feature. For information on this feature, see the *Cisco IOS Flexible NetFlow Features Roadmap*.

Examples

The following example shows how to configure an autonomous system aggregation scheme:

```
ipv6 flow-aggregation cache as
```

The following example shows how to configure multiple NetFlow export destinations on an aggregation cache:

```
ipv6 flow-aggregation cache destination-prefix
  export destination 2001::FFFE/64 9991
  export destination 2001::FFFC/64 1999
```

Related Commands

Command	Description
show ipv6 flow cache aggregation	Displays the IPv6 aggregation cache configuration.

ipv6 flow-cache entries

Note Effective with Cisco IOS Release 12.4(20)T, the **ipv6 flow-cache entries** command is not available in Cisco software.

To change the number of entries maintained in the NetFlow cache, use the **ipv6 flow-cache entries** command in global configuration mode. To return to the default number of entries, use the **no** form of this command.

ipv6 flow-cache entries *number*

no ipv6 flow-cache entries

Syntax Description

number	Number of entries to maintain in the NetFlow cache. The valid range is from 1024 to 524288 entries. The default is 65536 entries (64K).

Command Default

The default entry is used.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)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.
12.4(20)T	This command was removed.

Usage Guidelines

Normally the default size of the NetFlow cache will meet your needs. However, you can increase or decrease the number of entries maintained in the cache to meet the needs of your flow traffic rates. For environments with a high amount of flow traffic (such as an internet core router), a larger value such as 131072 (128K) is recommended. To obtain information on your flow traffic, use the **show ipv6 flow cache** command in privileged EXEC mode.

The default is 64K flow cache entries. Each cache entry is approximately 64 bytes of storage. Assuming a cache with the default number of entries, approximately 4 MB of DRAM would be required. Each time a new flow is taken from the free flow queue, the number of free flows is checked. If only a few free flows remain, NetFlow attempts to age 30 flows using an accelerated timeout. If only one free flow remains, NetFlow automatically ages 30 flows regardless of their age. The intent is to ensure that free flow entries are always available.

Caution Cisco recommends that you do not change the NetFlow cache entries. To return to the default NetFlow cache entries, use the **no ipv6 flow-cache entries** global configuration command.

Note The NetFlow for IPv6 feature has been replaced by the IPv6 Flexible NetFlow feature. For information on this feature, see the *Cisco IOS Flexible NetFlow Features Roadmap*.

Examples

The following example shows how to increase the number of entries in the NetFlow cache to 131,072 (128K):

```
Router(config)# ipv6 flow-cache entries 131072
```

Related Commands

Command	Description
cache	Configures the aggregation cache operational parameters.
show ipv6 flow cache	Displays the cache flow statistics for IPv6 flows.

ipv6 flow-cache timeout

Note Effective with Cisco IOS Release 12.4(20)T, the **ipv6 flow-cache timeout** command is not available in Cisco software.

To change the timeout values for the NetFlow cache, use the **ipv6 flow-cache timeout** command in global configuration mode. To return the timeout to the default values, use the **no** form of this command.

ipv6 flow-cache timeout {**active** *minutes* | **inactive** *seconds*}

no ipv6 flow-cache timeout

Syntax Description

active *minutes*	(Optional) Specifies the number of minutes that an active entry is active. The range is from 1 to 60 minutes. The default is 30 minutes.
inactive *seconds*	(Optional) Specifies the number of seconds that an inactive entry will stay in the aggregation cache before it times out. The range is from 10 to 600 seconds. The default is 15 seconds.

Command Default

The timeout default values are used.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)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.
12.4(20)T	This command was removed.

Examples

The following example shows how to adjust the timeout values. In this case, the active minutes are not specified so they remain at the default; the inactive seconds are set to 199.

```
ipv6 flow-cache timeout inactive 199
```

Note The NetFlow for IPv6 feature has been replaced by the IPv6 Flexible NetFlow feature. For information on this feature, see the *Cisco IOS Flexible NetFlow Features Roadmap*.

Related Commands

Command	Description
default-name	Enables an aggregation cache.
ipv6 flow-aggregation cache	Configures aggregation cache configuration scheme for NetFlow V9 for IPv6.
show ipv6 flow cache	Displays the IPv6 NetFlow cache, which is a table of current flows being fast-switched through the router.
show ipv6 cache flow aggregation	Displays the aggregation cache configuration.

ipv6 flow-export destination

Note Effective with Cisco IOS Release 12.4(20)T, the **ipv6 flow-export destination** command is not available in Cisco software.

To enable the exporting of information in NetFlow cache entries to a specific address or port, use the **ipv6 flow-export destination** command in global configuration mode. To disable the exporting of information, use the **no** form of this command.

ipv6 flow-export destination *ip-address udp-port*

no ipv6 flow-export destination *ip-address udp-port*

Syntax Description

ip-address	IPv4 address of the workstation to which you want to send the NetFlow information. IPv4 addresses only are supported as transport.
udp-port	User Datagram Protocol (UDP) protocol-specific port number.

Command Default

This command is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)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.
12.4(20)T	This command was removed.

Usage Guidelines

To configure multiple NetFlow export destinations to a networking device, enter the **ipv6 flow-export destination** command twice—once for each destination. Do not enter the same IPv4 address twice. However, entering two different IPv4 addresses with the same UDP port number is configurable.

A NetFlow cache entry contains a great deal of information. When NetFlow is enabled, you can use the **ipv6 flow-export destination** command to configure the networking device to export the flow cache entry to a workstation when a flow expires. This command can be useful for purposes of gathering information about statistics, billing, and security.

Note The NetFlow for IPv6 feature has been replaced by the IPv6 Flexible NetFlow feature. For information on this feature, see the *Cisco IOS Flexible NetFlow Features Roadmap*.

Examples

The following example shows how to configure the networking device to export the NetFlow cache entry to multiple export destinations:

```
ipv6 flow-export destination 10.42.42.1 9991
ipv6 flow-export destination 10.0.101.254 9991
```

Related Commands

Command	Description
ipv6 flow-aggregation cache	Configures aggregation cache configuration scheme for NetFlow V9 for IPv6.
show ipv6 flow cache aggregation	Displays the IPv6 NetFlow cache, which is a table of current flows being fast-switched through the router.

ipv6 flow-export source

Note Effective with Cisco IOS Release 12.4(20)T, the **ipv6 flow-export source** command is not available in Cisco software.

To specify the source interface IPv6 address used in the NetFlow export datagram, use the **ipv6 flow-export source** command in global configuration mode. To remove the source address, use the **no** form of this command.

ipv6 flow-export source *interface*

no ipv6 flow-export source

Syntax Description

interface	Interface from which the router gets the source IP or IPv6 address for the packet.

Command Default

No source interface is specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)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.
12.4(20)T	This command was removed.

Usage Guidelines

This command specifies the interface that identifies the IPv4 address to which data is exported from the main IPv6 cache.

After you configure NetFlow data export, you can also specify the source interface used in the User Datagram Protocol (UDP) datagram that contains the export data. The NetFlow Collector on the workstation uses the IP address of the source interface to determine which router sent the information. The NetFlow Collector also performs Simple Network Management Protocol (SNMP) queries to the router using the IP address of the source interface. Because the IP address of the source interface can change (for example, the interface might flap so a different interface is used to send the data), Cisco recommends that you configure a loopback source interface. A loopback interface is always up and can respond to SNMP queries from the NetFlow Collector on the workstation.

Note The NetFlow for IPv6 feature has been replaced by the IPv6 Flexible NetFlow feature. For information on this feature, see the *Cisco IOS Flexible NetFlow Features Roadmap*.

Examples

The following example shows the configuration for a loopback source interface. The loopback interface has the IP address 10.0.0.1:

```
Router# configure terminal
Router(config)# interface loopback0
Router(config-if)# ip address 10.0.0.1
Router(config-if)# exit
Router(config-if)# ip unnumbered loopback0
Router(config-if)# no ip mroute-cache
Router(config-if)# encapsulation ppp
Router(config-if)# ipv6 flow cache
Router(config-if)# exit
Router(config)# ipv6 flow-export source loopback0
Router(config)# exit
```

Related Commands

Command	Description
ipv6 flow-cache export destination	Enables the exporting of information in NetFlow cache entries.

ipv6 flow-export template

Note Effective with Cisco IOS Release 12.4(20)T, the **ipv6 flow-export template** command is not available in Cisco software.

To enable the exporting of information in NetFlow cache entries, use the **ipv6 flow-export template** command in global configuration mode. To disable the exporting of information, use the **no** form of this command.

ipv6 flow-export template {**refresh-rate** *packet-refresh-rate* | **timeout** *timeout-value*}

no ipv6 flow-export template

Syntax Description

refresh-rate *packet-refresh-rate*	Specifies the number of packets between cache refreshes. Value is from 1 to 600 packets.
timeout *timeout-value*	Specifies the length of time to wait before the export time is up. Value is 1 to 3600 minutes.

Command Default

No template is defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)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.
12.4(20)T	This command was removed.

Examples

The following example specifies that the NetFlow cache is refreshed after 150 packets are collected:

```
Router(config)# ipv6 flow-export template refresh-rate 150
```

Note The NetFlow for IPv6 feature has been replaced by the IPv6 Flexible NetFlow feature. For information on this feature, see the *Cisco IOS Flexible NetFlow Features Roadmap*.

Related Commands

Command	Description
ipv6 flow-aggregation cache	Configures aggregation cache configuration scheme for NetFlow V9 for IPv6.

ipv6 flow-export template options

Note Effective with Cisco IOS Release 12.4(20)T, the **ipv6 flow-export template options** command is not available in Cisco software.

To configure templates for IPv6 cache exports, use the **ipv6 flow-export template options** command in global configuration mode. To remove the template options from the NetFlow cache exports, use the **no** form of this command.

ipv6 flow-export template options {**export-stats** | **refresh-rate** *packet-refresh-rate* | **timeout** *timeout-value*}

no ipv6 flow-export template options

Syntax Description

export-stats	Exports the specified statistics.
refresh-rate *packet-refresh-rate*	Specifies the number of packets between cache refreshes. Value is from 1 to 600 packets.
timeout *timeout-value*	Specifies the length of time to wait before the export time is up. Value is 1 to 3600 minutes.

Command Default

No template is applied for flow exports.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)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.
12.4(20)T	This command was removed.

Usage Guidelines

A NetFlow cache entry contains a great deal of information. When flow switching is enabled, you can use the **ipv6 flow-export template options** command to configure the router to export the flow cache entry to a workstation when a flow expires.

Note The NetFlow for IPv6 feature has been replaced by the IPv6 Flexible NetFlow feature. For information on this feature, see the *Cisco IOS Flexible NetFlow Features Roadmap*.

Examples

The following example shows the configuration for a loopback source interface. The loopback interface has the IP address 10.10.0.1 and is used by the serial interface in slot 5, port 0.

```
Router# configure terminal
Router(config)# interface loopback0
Router(config-if)# ipv6 address 2001:0DB8:1:1:FFFF:FFFF:FFFF:FFFE/64
Router(config-if)# exit
Router(config)# interface serial 5/0:0
Router(config-if)# ip unnumbered loopback0
Router(config-if)# no ip mroute-cache
Router(config-if)# encapsulation ppp
Router(config-if)# ipv6 flow cache
Router(config-if)# exit
Router(config)# ipv6 flow-export source loopback0
Router(config)# exit
```

Related Commands

Command	Description
ipv6 flow-cache entries	Enables the exporting of information in NetFlow cache entries.

ipv6 flow-export version 9

Note Effective with Cisco IOS Release 12.4(20)T, the **ipv6 flow-export version 9** command is not available in Cisco software.

To enable the exporting of information in NetFlow cache entries, use the **ipv6 flow-export version 9** command in global configuration mode. To disable the exporting of information, use the **no** form of this command.

ipv6 flow-export version 9 [**origin-as** | **peer-as**] [**bgp-nexthop**]

no ipv6 flow-export version 9

Syntax Description

origin-as	(Optional) Specifies that export statistics include the origin autonomous system for the source and destination.
peer-as	(Optional) Specifies that export statistics include the peer autonomous system for the source and destination.
bgp-nexthop	(Optional) Specifies that export statistics be collected for the next Border Gateway Protocol (BGP) hop.

Command Default

The default is version 9 export.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)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.
12.4(20)T	This command was removed.

Usage Guidelines

NetFlow cache entries contain a great deal of information. When flow switching is enabled, you can use the **ipv6 flow-export version 9** command to configure the router to export the flow cache entry to a workstation when a flow expires. This command can be useful for purposes of gathering information about statistics, billing, and security.

Note The NetFlow for IPv6 feature has been replaced by the IPv6 Flexible NetFlow feature. For information on this feature, see the *Cisco IOS Flexible NetFlow Features Roadmap*.

Examples

The following example configures the router to collect information about the next BGP hop in the destination path:

```
ipv6 flow-export version 9 bgp-nexthop
```

Related Commands

Command	Description
ipv6 flow-aggregation cache	Configures the aggregation cache configuration scheme for NetFlow V9 for IPv6.

ipv6 flowset

To configure flow-label marking in 1280-byte or larger packets sent by the router, use the **ipv6 flowset** command in global configuration mode. To remove flow-label marking from packets, use the **no** form of this command.

ipv6 flowset

no ipv6 flowset

Syntax Description

This command has no arguments or keywords.

Command Default

Flow-label setting is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.

Usage Guidelines

The **ipv6 flowset** command configures the router to track destinations to which the router has sent packets that are 1280 bytes or larger. The command configures such a destination to be added to the router's MTU cache and tracked. The router then will accept toobig messages only if they relate to a tracked destinations to which the router has sent packets within the last two minutes.

Examples

The following example configures the router to track destinations to which it has sent packets that are 1280 bytes or larger:

```
Router(config)# ipv6 flowset
```

Related Commands

Command	Description
clear ipv6 mtu	Clears the MTU cache of messages.

ipv6 general-prefix

To define an IPv6 general prefix, use the **ipv6 general-prefix** command in global configuration mode. To remove the IPv6 general prefix, use the **no** form of this command.

ipv6 general-prefix *prefix-name* {*ipv6-prefix*/*prefix-length* | **6to4** *interface-type interface-number* | **6rd** *interface-type interface-number*}

no ipv6 general-prefix *prefix-name*

Syntax Description

prefix-name	The name assigned to the prefix.
ipv6-prefix	The IPv6 network assigned to the general prefix. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons. When defining a general prefix manually, specify both the *ipv6-prefix* and */prefix-length* arguments.
/prefix-length	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value. When defining a general prefix manually, specify both the *ipv6-prefix* and */prefix-length* arguments.
6to4	Allows configuration of a general prefix based on an interface used for 6to4 tunneling. When defining a general prefix based on a 6to4 interface, specify the **6to4** keyword and the *interface-type interface-number* argument.
interface-type interface-number	Interface type and number. For more information, use the question mark (**?**) online help function. When defining a general prefix based on a 6to4 interface, specify the **6to4** keyword and the *interface-type interface-number* argument.
6rd	Allows configuration of a general prefix computed from an interface used for IPv6 rapid deployment (6RD) tunneling.

Command Default

No general prefix is defined.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Release	Modification
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
Cisco IOS XE Release 3.1S	The optional **6rd** keyword was added.

Usage Guidelines

Use the **ipv6 general-prefix** command to define an IPv6 general prefix.

A general prefix holds a short prefix, based on which a number of longer, more specific, prefixes can be defined. When the general prefix is changed, all of the more specific prefixes based on it will change, too. This function greatly simplifies network renumbering and allows for automated prefix definition.

More specific prefixes, based on a general prefix, can be used when configuring IPv6 on an interface.

When defining a general prefix based on an interface used for 6to4 tunneling, the general prefix will be of the form 2002:a.b.c.d::/48, where “a.b.c.d” is the IPv4 address of the interface referenced.

Examples

The following example manually defines an IPv6 general prefix named my-prefix:

```
Router(config)# ipv6 general-prefix my-prefix 2001:DB8:2222::/48
```

The following example defines an IPv6 general prefix named my-prefix based on a 6to4 interface:

```
Router(config)# ipv6 general-prefix my-prefix 6to4 ethernet0
```

Related Commands

Command	Description
show ipv6 general-prefix	Displays information on general prefixes for an IPv6 addresses.

ipv6 hello-interval eigrp

To configure the hello interval for the Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 routing process designated by an autonomous system number, use the **ipv6 hello-interval eigrp** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ipv6 hello-interval eigrp *as-number seconds*

no ipv6 hello-interval eigrp *as-number seconds*

Syntax Description

as-number	Autonomous system number.
seconds	Hello interval, in seconds. The range is from 1 to 65535.

Command Default

For low-speed, nonbroadcast multiaccess (NBMA) networks, the default hello interval is 60 seconds. For all other networks, the default hello interval is 5 seconds.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(6)T	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.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

The default of 60 seconds applies only to low-speed, NBMA media. Low speed is considered to be a rate of T1 or slower, as specified with the **bandwidth** interface configuration command. Note that for the purposes of EIGRP for IPv6, Frame Relay and Switched Multimegabit Data Service (SMDS) networks may be considered to be NBMA. These networks are considered NBMA if the interface has not been configured to use physical multicasting; otherwise, they are considered not to be NBMA.

Examples

The following example sets the hello interval for Ethernet interface 0 to 10 seconds on autonomous system 1:

```
interface ethernet 0
 ipv6 hello-interval eigrp 1 10
```

Related Commands

Command	Description
bandwidth (interface)	Sets a bandwidth value for an interface.
ipv6 hold-time eigrp	Configures the hold time for a particular EIGRP for IPv6 routing process designated by the autonomous system number.

ipv6 hold-time eigrp

To configure the hold time for a particular Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 routing process designated by the autonomous system number, use the **ipv6 hold-time eigrp** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ipv6 hold-time eigrp *as-number seconds*

no ipv6 hold-time eigrp *as-number seconds*

Syntax Description

as-number	Autonomous system number.
seconds	Hello interval, in seconds. The range is from 1 to 65535.

Command Default

For low-speed, nonbroadcast multiaccess (NBMA) networks, the default hold-time interval is 180 seconds.
For all other networks, the default hold-time interval is 15 seconds.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(6)T	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.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

On very congested and large networks, the default hold time might not be sufficient time for all routers and access servers to receive hello packets from their neighbors. In this case, you may want to increase the hold time.

Cisco recommends that the hold time be at least three times the hello interval. If a router does not receive a hello packet within the specified hold time, routes through this router are considered unavailable.

Increasing the hold time delays route convergence across the network.

The default of 180 seconds hold time and 60 seconds hello interval apply only to low-speed, NBMA media. Low speed is considered to be a rate of T1 or slower, as specified with the **bandwidth** command.

Examples

The following example sets the hold time for Ethernet interface 0 to 40 seconds for AS 1:

```
interface ethernet 0
 ipv6 hold-time eigrp 1 40
```

Related Commands

Command	Description
bandwidth (interface)	Sets a bandwidth value for an interface.
ipv6 hello-interval eigrp	Configures the hello interval for the EIGRP for IPv6 routing process designated by an autonomous system number.

ipv6 hop-limit

To configure the maximum number of hops used in router advertisements and all IPv6 packets that are originated by the router, use the **ipv6 hop-limit** command in global configuration mode. To return the hop limit to its default value, use the **no** form of this command.

ipv6 hop-limit *value*

no ipv6 hop-limit *value*

Syntax Description

value	The maximum number of hops. The acceptable range is from 1 to 255.

Command Default

The default is 64 hops.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)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 Release 12.2(14)S.
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.
12.2(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 configures a maximum number of 15 hops for router advertisements and all IPv6 packets that are originated from the router:

```
Router(config)# ipv6 hop-limit 15
```

ipv6 host

To define a static host name-to-address mapping in the host name cache, use the **ipv6 host** command in global configuration mode. To remove the host name-to-address mapping, use the **no** form of this command.

ipv6 host *name* [*port*] *ipv6-address1* [*ipv6-address2...ipv6-address4*]

no ipv6 host *name*

Syntax Description

name	Name of the IPv6 host. The first character can be either a letter or a number. If you use a number, the operations you can perform are limited.
port	(Optional) The default Telnet port number for the associated IPv6 addresses.
ipv6-address1	Associated IPv6 address. 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-address2... ipv6-.address4	(Optional) Additional associated IPv6 addresses. You can bind up to four addresses to a host name.

Command Default

Static host name-to-address mapping in the host name cache is not defined.
The default Telnet port is 23.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)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 Release 12.2(14)S.
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.
12.2(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 **ipv6 host** command is similar to the **ip host** command, except that it is IPv6-specific.

The first character of the name can be either a letter or a number. If you use a number, the operations you can perform (such as **ping**) are limited.

Examples

The following example defines two static mappings:

```
Router(config)# ipv6 host cisco-sj 2001:0DB8:1::12
Router(config)# ipv6 host cisco-hq 2002:C01F:768::1 2001:0DB8:1::12
```

Related Commands

Command	Description
show hosts	Displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of host names and addresses.

ipv6 icmp error-interval

To configure the interval and bucket size for IPv6 Internet Control Message Protocol (ICMP) error messages, use the **ipv6 icmp error-interval** command in global configuration mode. To return the interval to its default setting, use the **no** form of this command.

ipv6 icmp error-interval *milliseconds* [*bucketsize*]

no ipv6 icmp error-interval

Syntax Description

milliseconds	The time interval between tokens being placed in the bucket. The acceptable range is from 0 to 2147483647 with a default of 100 milliseconds.
bucketsize	(Optional) The maximum number of tokens stored in the bucket. The acceptable range is from 1 to 200 with a default of 10 tokens.

Command Default

ICMP rate limiting is enabled by default. To disable ICMP rate limiting, set the interval to zero.
The time interval between tokens placed in the bucket is 100 milliseconds.
The maximum number of tokens stored in the bucket is 10.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(8)T	Support for IPv6 ICMP rate limiting was extended to use token buckets.
12.0(21)ST	This command, without the extension to use token buckets, was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command, without the extension to use token buckets, was integrated into Cisco IOS Release 12.0(22)S.
12.0(23)S	This command, with the support for IPv6 ICMP rate limiting extended to use token buckets, was integrated into Cisco IOS Release 12.0(23)S.
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.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
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

Use the **ipv6 icmp error-interval** command to limit the rate at which IPv6 ICMP error messages are sent. A token bucket algorithm is used with one token representing one IPv6 ICMP error message. Tokens are placed in the virtual bucket at a specified interval until the maximum number of tokens allowed in the bucket is reached.

The *milliseconds* argument specifies the time interval between tokens arriving in the bucket. The optional *bucketsize* argument is used to define the maximum number of tokens allowed in the bucket. Tokens are removed from the bucket when IPv6 ICMP error messages are sent, which means that if the *bucketsize* is set to 20, a rapid succession of 20 IPv6 ICMP error messages can be sent. When the bucket is empty of tokens, IPv6 ICMP error messages are not sent until a new token is placed in the bucket.

Use the **show ipv6 traffic** command to display IPv6 ICMP rate-limited counters.

Examples

The following example shows an interval of 50 milliseconds and a bucket size of 20 tokens being configured for IPv6 ICMP error messages:

```
ipv6 icmp error-interval 50 20
```

Related Commands

Command	Description
show ipv6 traffic	Displays statistics about IPv6 traffic.

ipv6 inspect

To apply a set of inspection rules to an interface, use the **ipv6 inspect** command in interface configuration mode. To remove the set of rules from the interface, use the **no** form of this command.

ipv6 inspect *inspection-name* {**in** | **out**}

no ipv6 inspect *inspection-name* {**in** | **out**}

Syntax Description

inspection-name	Identifies which set of inspection rules to apply.
in	Applies the inspection rules to inbound traffic.
out	Applies the inspection rules to outbound traffic.

Command Default

If no set of inspection rules is applied to an interface, no traffic will be inspected by Context-Based Access Control (CBAC).

Command Modes

Interface configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

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.

If you apply the rules to outbound traffic, then return inbound packets will be permitted if they belong to a valid connection with existing state information. This connection must be initiated with an outbound packet.

If you apply the rules to inbound traffic, then return outbound packets will be permitted if they belong to a valid connection with existing state information. This connection must be initiated with an inbound packet.

Examples

The following example applies a set of inspection rules named “outboundrules” to an external interface’s outbound traffic. This causes 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
 ipv6 inspect outboundrules out
```

Related Commands

Command	Description
ipv6 inspect name	Defines a set of inspection rules.

ipv6 inspect alert-off

To disable Context-based Access Control (CBAC) alert messages, which are displayed on the console, use the **ipv6 inspect alert off** command in global configuration mode. To enable Cisco IOS firewall alert messages, use the **no** form of this command.

ipv6 inspect alert-off

no ipv6 inspect alert-off

Syntax Description

This command has no arguments or keywords.

Command Default

Alert messages are displayed.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Examples

The following example turns off CBAC alert messages:

```
ipv6 inspect alert-off
```

Related Commands

Command	Description
ipv6 inspect audit trail	Turns on CBAC audit trail messages, which will be displayed on the console after each CBAC session close.
ipv6 inspect name	Applies a set of inspection rules to an interface.

ipv6 inspect audit trail

To turn on Context-based Access Control (CBAC) audit trail messages, which will be displayed on the console after each Cisco IOS firewall session closes, use the **ipv6 inspect audit trail** command in global configuration mode. To turn off Cisco IOS firewall audit trail message, use the **no** form of this command.

ipv6 inspect audit trail

no ipv6 inspect audit trail

Syntax Description

This command has no arguments or keywords.

Command Default

Audit trail messages are not displayed.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

Use this command to turn on CBAC audit trail messages.

Examples

The following example turns on CBAC audit trail messages:

```
ipv6 inspect audit trail
```

Afterward, audit trail messages such as the following are displayed:

```
%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
```

These messages are examples of audit trail messages. To determine which protocol was inspected, refer to the responder's port number. The port number follows the responder's IP address.

Related Commands

Command	Description
ipv6 inspect alert-off	Disables CBAC alert messages.
ipv6 inspect name	Applies a set of inspection rules to an interface.

ipv6 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 **ipv6 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.

ipv6 inspect max-incomplete high *number*

no ipv6 inspect max-incomplete 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. The value range is 1 through 4294967295.

Command Default

The default is 500 half-open sessions.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

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, “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:

```
ipv6 inspect max-incomplete high 900
ipv6 inspect max-incomplete low 800
```

Related Commands

Command	Description
ipv6 inspect max-incomplete low	Defines the number of existing half-open sessions that will cause the software to stop deleting half-open sessions.
ipv6 inspect one-minute high	Defines the rate of new unestablished sessions that will cause the software to start deleting half-open sessions.
ipv6 inspect one-minute low	Defines the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions.
ipv6 inspect tcp max-incomplete host	Specifies the threshold and blocking time values for TCP host-specific denial-of-service detection and prevention.

ipv6 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 **ipv6 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.

ipv6 inspect max-incomplete low *number*

no ipv6 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. Value range is 1 through 4294967295.

Command Default

The default is 400 half-open sessions.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

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, “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:

```
ipv6 inspect max-incomplete high 900
ipv6 inspect max-incomplete low 800
```

Related Commands

Command	Description
ipv6 inspect max-incomplete high	Defines the number of existing half-open sessions that will cause the software to start deleting half-open sessions.
ipv6 inspect one-minute high	Defines the rate of new unestablished sessions that will cause the software to start deleting half-open sessions.
ipv6 inspect one-minute low	Defines the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions.
ipv6 inspect tcp max-incomplete host	Specifies the threshold and blocking time values for TCP host-specific denial-of-service detection and prevention.

ipv6 inspect name

To define a set of ipv6 inspection rules, use the **ipv6 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.

ipv6 inspect name *inspection-name protocol* [**alert** {**on** | **off**}] [**audit-trail** {**on** | **off**}] [**timeout** *seconds*]

no ipv6 inspect name *inspection-name* [*protocol*]

Syntax Description

inspection-name	Names 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.
protocol	A specified protocol. Possible protocol values are **icmp**, **udp**, **tcp**, and **ftp**. This value is optional in the **no** version of this command.
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 based on the setting of the **ipv6 inspect alert-off** command.
audit-trail {**on** | **off**}	(Optional) For each inspected protocol, the audit trail can be set on or off. If no option is selected, audit trail messages are generated based on the setting of the **ipv6 inspect audit-trail** command.
timeout *seconds*	(Optional) Specifies the number of seconds for a different idle timeout to override the global TCP or User Datagram Protocol (UDP) idle timeouts for the specified protocol. This timeout overrides the global TCP and UPD timeouts but will not override the global Domain Name System (DNS) timeout.
timeout *seconds* (fragmentation)	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 than 1 second, it will be 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 less than 32, the timeout will be divided by 2. When the number of free states is less than 16, the timeout will be set to 1 second.

Command Default

No set of inspection rules is defined.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.3(11)T	FTP protocol support was added.

Usage Guidelines

To define a set of inspection rules, enter this 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 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.

To define a single set of inspection rules, configure inspection for all the desired application-layer protocols, and for TCP, UDP, or Internet Control Message Protocol (ICMP) 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 named inspection rules, use the **no** form of this command with the specified inspection name.

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.

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.

ICMP Inspection

An ICMP inspection session is on the basis of the source address of the inside host that originates the ICMP packet. Dynamic access control lists (ACLs) are created for return ICMP packets of the allowed types (destination unreachable, echo-reply, time-exceeded, and packet too big) for each session. There are no port numbers associated with an ICMP session, and the permitted IP address of the return packet is wild-carded in the ACL. The wild-card 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.

FTP Inspection

Cisco IOS Firewall uses layer 7 support for application modules such as FTP.

Cisco IOS IPv6 Firewall uses RFC 2428 to garner IPv6 addresses and corresponding ports. If an address other than an IPv6 address is present, the FTP data channel is not opened.

IPv6-specific port-to-application mapping (PAM) provides FTP inspection. PAM translates TCP or UDP port numbers into specific network services or applications. By mapping port numbers to network services or applications, an administrator can force firewall inspection on custom configurations not defined by well-known ports. PAM delivers with the standard well-known ports defined as defaults.

Table 31 describes the transport-layer and network-layer protocols.

Table 31 Protocol Keywords—Transport-Layer and Network-Layer Protocols

Protocol	Keyword
ICMP	**icmp**
TCP	**tcp**
UDP	**udp**
FTP	**ftp**

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-carded 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 hole 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.

Examples

The following example causes the software to inspect TCP sessions and UDP sessions:

```
ipv6 inspect name myrules tcp
ipv6 inspect name myrules udp audit-trail on
```

Related Commands

Command	Description
ipv6 inspect alert-off	Disables CBAC alert messages.
ipv6 inspect audit trail	Turns on CBAC audit trail messages, which will be displayed on the console after each CBAC session close.

ipv6 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 **ipv6 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.

ipv6 inspect one-minute high *number*

no ipv6 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. Value range is 1 through 4294967295

Command Default

The default is 500 half-open sessions.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

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, “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:

```
ipv6 inspect one-minute high 1000
ipv6 inspect one-minute low 950
```

Related Commands

Command	Description
ipv6 inspect one-minute low	Defines the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions.
ipv6 inspect max-incomplete high	Defines the number of existing half-open sessions that will cause the software to start deleting half-open sessions.
ipv6 inspect max-incomplete low	Defines the number of existing half-open sessions that will cause the software to stop deleting half-open sessions.
ipv6 inspect tcp max-incomplete host	Specifies the threshold and blocking time values for TCP host-specific denial-of-service detection and prevention.

ipv6 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 **ipv6 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.

ipv6 inspect one-minute low *number*

no ipv6 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. Value range is 1 through 4294967295.

Command Default

The default is 400 half-open sessions.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

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, “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:

```
ipv6 inspect one-minute high 1000
ipv6 inspect one-minute low 950
```

Related Commands

Command	Description
ipv6 inspect max-incomplete high	Defines the number of existing half-open sessions that will cause the software to start deleting half-open sessions.
ipv6 inspect max-incomplete low	Defines the number of existing half-open sessions that will cause the software to stop deleting half-open sessions.
ipv6 inspect one-minute high	Defines the rate of new unestablished sessions that will cause the software to start deleting half-open sessions.
ipv6 inspect tcp max-incomplete host	Specifies the threshold and blocking time values for TCP host-specific denial-of-service detection and prevention.

ipv6 inspect routing-header

To specify whether Context-based Access Control (CBAC) should inspect packets containing an IPv6 routing header, use the **ipv6 inspect routing-header** command. To drop packets containing an IPv6 routing header, use the **no** form of this command.

ipv6 inspect routing-header

no ipv6 inspect routing-header

Syntax Description

This command has no arguments or keywords.

Command Default

Packets containing IPv6 routing header are dropped.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

An IPv6 source uses the routing header to list one or more intermediate nodes to be visited between the source and destination of the packet. The Cisco IOS firewall uses this header to retrieve the destination host address. Cisco IOS firewall will establish the appropriate inspection session based on the retrieved address from the routing header.

The originating node lists all intermediate nodes that the packet must traverse. The source and destination address pair in the IPv6 header identifies the hop between the originating node and the first intermediate node. Once the first intermediate node receives the packet, it looks for a routing header. If the routing header is present, the next intermediate node address is swapped with the destination address in the IPv6 header and the packet is forwarded to the next intermediate node. This sequence continues for each intermediate node listed in the routing until no more entries exist in the routing header. The last entry in the routing header is the final destination address.

Examples

The following example causes the software to inspect TCP sessions and UDP sessions:

```
ip inspect routing-header
```

Related Commands

Command	Description
ipv6 inspect alert-off	Disables CBAC alert messages.
ipv6 inspect audit trail	Turns on CBAC audit trail messages, which will be displayed on the console after each CBAC session close.
ipv6 inspect name	Applies a set of inspection rules to an interface.

ipv6 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 **ipv6 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.

ipv6 inspect tcp idle-time *seconds*

no ipv6 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).

Command Default

The default is 3600 seconds (1 hour)

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

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 **ipv6 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):

```
ipv6 inspect tcp idle-time 1800
```

The following example sets the global TCP idle timeout back to the default of 3600 seconds (one hour):

```
no ipv6 inspect tcp idle-time
```

Related Commands

Command	Description
ipv6 inspect name	Defines a set of IPv6 inspection rules.

ipv6 inspect tcp max-incomplete host

To specify threshold and blocking time values for TCP host-specific denial-of-service detection and prevention, use the **ipv6 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.

ipv6 inspect tcp max-incomplete host *number* **block-time** *minutes*

no ipv6 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. Value range is 1 through 4294967295
block-time	Specifies blocking of connection initiation to a host. Value range is 0 through 35791.
minutes	Specifies how long the software will continue to delete new connection requests to the host. The default is 0 minutes.

Command Default

The default is 50 half-open sessions and 0 minutes.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

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 (120 seconds):

```
ipv6 inspect tcp max-incomplete host 40 block-time 120
```

The following example resets the defaults (50 half-open sessions and 0 seconds):

```
no ipv6 inspect tcp max-incomplete host
```

Related Commands

Command	Description
ipv6 inspect max-incomplete high	Defines the number of existing half-open sessions that will cause the software to start deleting half-open sessions.
ipv6 inspect max-incomplete low	Defines the number of existing half-open sessions that will cause the software to stop deleting half-open sessions.
ipv6 inspect one-minute high	Defines the rate of new unestablished sessions that will cause the software to start deleting half-open sessions.
ipv6 inspect one-minute low	Defines the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions.

ipv6 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 **ipv6 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.

ipv6 inspect tcp synwait-time *seconds*

no ipv6 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. Value range is 1 through 2147483

Command Default

The default is 30 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

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 session's first SYN bit 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:

```
ipv6 inspect tcp synwait-time 20
```

The following example changes the "synwait" timeout back to the default (30 seconds):

```
no ipv6 inspect tcp synwait-time
```

Related Commands

Command	Description
ipv6 inspect udp idle-time	Specifies the User Datagram Protocol idle timeout (the length of time for which a UDP "session" will still be managed while there is no activity).

ipv6 inspect udp idle-time

To specify the User Datagram Protocol idle timeout (the length of time for which a UDP "session" will still be managed while there is no activity), use the **ipv6 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.

ipv6 inspect udp idle-time *seconds*

no ipv6 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. Value range is 1 through 2147483

Command Default

The default is 30 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

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 **ipv6 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):

```
ipv6 inspect udp idle-time 120
```

The following example sets the global UDP idle timeout back to the default of 30 seconds:

```
no ipv6 inspect udp idle-time
```

ipv6 local policy route-map

To configure policy-based routing (PBR) for IPv6 for packets generated by the router, use the **ipv6 local policy route-map** command in global configuration mode. To disable local policy routing, use the **no** form of this command.

ipv6 local policy route-map *route-map-name*

no ipv6 local policy route-map *route-map-name*

Syntax Description

route-map-name	Name of the route map to use for local PBR. The name must match a *route-map-name* value specified by a **route-map** command.

Command Default

Packets that are generated by the router are not policy routed.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)S.
12.2(33)SXI4	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SXI4.
Cisco IOS XE Release 3.2S	This command was modified. It was integrated into Cisco IOS XE Release 3.2S.

Usage Guidelines

Packets that are generated by the router are not normally policy routed. However, you can use the **ipv6 local policy route-map** command to policy route such packets. You might enable local PBR if you want packets originated at the router to take a route other than the obvious shortest path.

The **ipv6 local policy route-map** command identifies a route map to use for local PBR. The **route-map** commands each have a list of **match** and **set** commands associated with them. The **match** commands specify the match criteria, which are the conditions under which packets should be policy routed. The **set** commands specify the set actions, which are the particular policy routing actions to perform if the criteria enforced by the **match** commands are met. The **no ipv6 local policy route-map** command deletes the reference to the route map and disables local policy routing.

Examples

In the following example, packets with a destination IPv6 address matching that allowed by access list pbr-src-90 are sent to the router at IPv6 address 2003:1::95:

```
ipv6 access-list src-90
 permit ipv6 host 2003::90 2001:1000::/64

route-map pbr-src-90 permit 10
 match ipv6 address src-90
```

```
 set ipv6 next-hop 2003:1::95

ipv6 local policy route-map pbr-src-90
```

Related Commands

Command	Description
ipv6 policy route-map	Configures IPv6 PBR on an interface.
match ipv6 address	Specifies an IPv6 access list to use to match packets for PBR for IPv6.
match length	Bases policy routing on the Level 3 length of a packet.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or to enable policy routing.
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Indicates where to output packets that pass a match clause of a route map for policy routing.
set ipv6 default next-hop	Specifies an IPv6 default next hop to which matching packets will be forwarded.
set ipv6 next-hop (PBR)	Indicates where to output IPv6 packets that pass a match clause of a route map for policy routing.
set ipv6 precedence	Sets the precedence value in the IPv6 packet header.

ipv6 local pool

To configure a local IPv6 prefix pool, use the **ipv6 local pool** configuration command with the prefix pool name. To disband the pool, use the **no** form of this command.

ipv6 local pool *poolname prefix/prefix-length assigned-length* [**shared**] [**cache-size** *size*]

no ipv6 local pool *poolname*

Syntax Description

poolname	User-defined name for the local prefix pool.
prefix	IPv6 prefix assigned to the pool. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/prefix-length	The length of the IPv6 prefix assigned to the pool. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address).
assigned-length	Length of prefix, in bits, assigned to the user from the pool. The value of the *assigned-length* argument cannot be less than the value of the */prefix-length* argument.
shared	(Optional) Indicates that the pool is a shared pool.
cache-size *size*	(Optional) Specifies the size of the cache.

Command Default

No pool is configured.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

All pool names must be unique.

IPv6 prefix pools have a function similar to IPv4 address pools. Contrary to IPv4, a block of addresses (an address prefix) are assigned and not single addresses.

Prefix pools are not allowed to overlap.

Once a pool is configured, it cannot be changed. To change the configuration, the pool must be removed and recreated. All prefixes already allocated will also be freed.

Examples

This example shows the creation of an IPv6 prefix pool:

```
Router (config)# ipv6 local pool pool1 2001:0DB8::/29 64
Router# show ipv6 local pool

Pool Prefix Free In use
pool1  2001:0DB8::/29  65516  20
```

Related Commands

Command	Description
debug ipv6 pool	Enables IPv6 pool debugging.
peer default ipv6 address pool	Specifies the pool from which client prefixes are assigned for PPP links.
prefix-delegation pool	Specifies a named IPv6 local prefix pool from which prefixes are delegated to DHCP for IPv6 clients.
show ipv6 local pool	Displays information about any defined IPv6 address pools.

ipv6 mfib

To reenable IPv6 multicast forwarding on the router, use the **ipv6 mfib** command in global configuration mode. To disable IPv6 multicast forwarding on the router, use the **no** form of this command.

ipv6 mfib

no ipv6 mfib

Syntax Description

The command has no arguments or keywords.

Command Default

Multicast forwarding is enabled automatically when IPv6 multicast routing is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)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

After a user has enabled the **ipv6 multicast-routing** command, IPv6 multicast forwarding is enabled. Because IPv6 multicast forwarding is enabled by default, use the **no** form of the **ipv6 mfib** command to disable IPv6 multicast forwarding.

Examples

The following example disables multicast forwarding on the router:

```
no ipv6 mfib
```

Related Commands

Command	Description
ipv6 multicast-routing	Enables multicast routing using PIM and MLD on all IPv6-enabled interfaces of the router and enables multicast forwarding.

ipv6 mfib-cef

To enable Multicast Forwarding Information Base (MFIB) Cisco Express Forwarding-based (interrupt level) IPv6 multicast forwarding for outgoing packets on a specific interface, use the **ipv6 mfib-cef** command in interface configuration mode. To disable CEF-based IPv6 multicast forwarding, use the **no** form of this command.

ipv6 mfib-cef

no ipv6 mfib-cef

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(18)SXE	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

Cisco Express Forwarding-based (interrupt level) IPv6 multicast forwarding is enabled by default when you enable Cisco Express Forwarding-based IPv6 multicast routing.

Use the **show ipv6 mfib interface** command to display the multicast forwarding interface status.

Examples

This example shows how to enable Cisco Express Forwarding-based IPv6 multicast forwarding:

```
Router(config-if)# ipv6 mfib-cef
```

This example shows how to disable Cisco Express Forwarding-based IPv6 multicast forwarding:

```
Router(config-if)# no ipv6 mfib-cef
```

Related Commands

Command	Description
show ipv6 mfib interface	Displays information about IPv6 multicast-enabled interfaces and their forwarding status.

ipv6 mfib cef output

To enable Multicast Forwarding Information Base (MFIB) interrupt-level IPv6 multicast forwarding of outgoing packets on a specific interface, use the **ipv6 mfib cef output** command in interface configuration mode. To disable MFIB interrupt-level IPv6 multicast forwarding, use the **no** form of this command.

ipv6 mfib cef output

no ipv6 mfib cef output

Syntax Description

This command has no arguments or keywords.

Command Default

Cisco Express Forwarding-based forwarding is enabled by default on interfaces that support it.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)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

After a user has enabled the **ipv6 multicast-routing** command, MFIB interrupt switching is enabled to run on every interface. Use the **no** form of the **ipv6 mfib cef output** command to disable interrupt-switching on a specific interface.

Use the **show ipv6 mfib interface** command to display the multicast forwarding status of interfaces.

Examples

The following example disables MFIB interrupt switching on Fast Ethernet interface 1/0:

```
Router(config)# interface FastEthernet 1/0
Router(config-if)# no ipv6 mfib cef output
```

Related Commands

Command	Description
ipv6 multicast-routing	Enables multicast routing using PIM and MLD on all IPv6-enabled interfaces of the router and enables multicast forwarding.
show ipv6 mfib interface	Displays IPv6 multicast-enabled interfaces and their forwarding status.

ipv6 mfib fast

Note Effective in Cisco IOS Release 12.3(4)T, the **ipv6 mfib fast** command is replaced by the **ipv6 mfib cef output** command. See the **ipv6 mfib cef output** command for more information.

To enable Multicast Forwarding Information Base (MFIB) interrupt-level IPv6 multicast forwarding of outgoing packets on a specific interface, use the **ipv6 mfib fast** command in interface configuration mode. To disable MFIB interrupt-level IPv6 multicast forwarding, use the **no** form of this command.

ipv6 mfib fast

no ipv6 mfib fast

Syntax Description

This command has no arguments or keywords.

Command Default

Cisco Express Forwarding-based forwarding is enabled by default on interfaces that support it.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.3(4)T	The command was replaced by the **ipv6 mfib cef output** command.
12.2(25)S	The command was replaced by the **ipv6 mfib cef output** command.
12.0(28)S	The command was replaced by the **ipv6 mfib cef output** command.

Usage Guidelines

After a user has enabled the **ipv6 multicast-routing** command, MFIB interrupt switching is enabled to run on every interface. Use the **no** form of the **ipv6 mfib fast** command to disable interrupt-switching on a specific interface.

Use the **show ipv6 mfib interface** command to display the multicast forwarding status of interfaces.

Examples

The following example disables MFIB interrupt switching on Fast Ethernet interface 1/0:

```
Router(config)# interface FastEthernet 1/0
Router(config-if)# no ipv6 mfib fast
```

Related Commands

Command	Description
ipv6 multicast-routing	Enables multicast routing using PIM and MLD on all IPv6-enabled interfaces of the router and enables multicast forwarding.
show ipv6 mfib interface	Displays IPv6 multicast-enabled interfaces and their forwarding status.

ipv6 mfib forwarding

To enable IPv6 multicast forwarding of packets received from a specific interface on the router, use the **ipv6 mfib forwarding** command in interface configuration mode. To disable IPv6 multicast forwarding of packets received from a specific interface, use the **no** form of this command.

ipv6 mfib forwarding

no ipv6 mfib forwarding

Syntax Description

This command has no arguments or keywords.

Command Default

Multicast forwarding is enabled automatically when IPv6 multicast routing is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)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.

Usage Guidelines

The **no ipv6 mfib forwarding** command is used to disable multicast forwarding of packets received from a specified interface, although the specified interface on the router will still continue to receive multicast packets destined for applications on the router itself.

Because multicast forwarding is enabled automatically when IPv6 multicast routing is enabled, the **ipv6 mfib forwarding** command is used to reenable multicast forwarding of packets if it has been previously disabled.

Examples

The following example shows how to disable multicast forwarding of packets from Ethernet 1/1:

```
Router(config) interface Ethernet1/1
Router(config-if) no ipv6 mfib forwarding
```

Related Commands

Command	Description
ipv6 mfib	Reenables IPv6 multicast forwarding on the router.

ipv6 mfib hardware-switching

To configure Multicast Forwarding Information Base (MFIB) hardware switching for IPv6 multicast packets on a global basis, use the **ipv6 mfib hardware-switching** command in global configuration mode. To disable this function, use the **no** form of this command.

ipv6 mfib hardware-switching [**connected | issu-support | replication-mode ingress | shared-tree | uplink**]

no ipv6 mfib hardware-switching [**connected | issu-support | replication-mode ingress | shared-tree | uplink**]

Syntax Description

connected	(Optional) Allows you to download the interface and mask entry, and installs subnet entries in the access control list (ACL)-ternary content addressable memory (TCAM).
issu-support	(Optional) Enables In-Service Software Upgrade (ISSU) support for IPv6 multicast.
replication-mode ingress	(Optional) Sets the hardware replication mode to ingress.
shared-tree	(Optional) Sets the hardware switching for IPv6 multicast packets.
uplink	(Optional) Enables IPv6 multicast on the uplink ports of the Supervisor Engine 720-10GE.

Defaults

This command is enabled with the **connected** and **replication-mode ingress** keywords.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)SXE	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.
12.2(18)SXH	This command was modified. The **shared-tree** and the **uplink** keywords were added.
12.2(33)SXI	This command was modified. The **issu-support** keyword was added on the Supervisor Engine 4.
12.2(33)SXI2	This command was modified. The **issu-support** keyword was added on the Supervisor Engine 720 in distributed Cisco Express Forwarding (dCEF)-only mode.

Usage Guidelines

You must enter the **ipv6 mfib hardware-switching uplink** command to enable IPv6 multicast hardware switching on the standby Supervisor Engine 720-10GE.

Note The system message "PSTBY-2-CHUNKPARTIAL: Attempted to destroy partially full chunk, chunk 0xB263638, chunk name: MET FREE POOL" is displayed on the Supervisor Engine if both the **fabric switching-mode allow dcef-only** and **ipv6 mfib hardware-switching uplink** commands are configured. The router will ignore the command configured last.

The **ipv6 mfib hardware-switching uplink** command ensures support of IPv6 multicast on standby uplink ports on systems that are configured with a Supervisor Engine 720-10GE only. You must reboot the system for this command to take effect. The MET space is halved on both the supervisor engines and the C+ modules.

Enabling the **ipv6 mfib hardware-switching issu-support** command will consume one Switched Port Analyzer (SPAN) session. This command will be effective if the image versions on the active and standby supervisors are different. If the command is not enabled, then the IPv6 multicast traffic ingressing and egressing from standby uplinks will be affected. This command is NVGENed. This command should be configured only once and preferably before performing the In-Service Software Upgrade (ISSU) load version process.

Note After completing the ISSU process, the administrator should disable the configured **ipv6 mfib hardware-switching issu-support** command.

Examples

The following example shows how to prevent the installation of the subnet entries on a global basis:

```
Router(config)# ipv6 mfib hardware-switching
```

The following example shows how to set the hardware replication mode to ingress:

```
Router(config)# ipv6 mfib hardware-switching replication-mode ingress
```

The following example shows how to enable IPv6 multicast on standby uplink ports on systems that are configured with a Supervisor Engine 720-10GE only:

```
Router(config)# ipv6 mfib hardware-switching uplink
Router(config)# end
Router# reload
```

Related Commands

Command	Description
fabric switching-mode allow dcef-only	Enables the truncated mode in the presence of two or more fabric-enabled switching modules.
show platform software ipv6-multicast	Displays information about the platform software for IPv6 multicast.

ipv6 mfib-mode centralized-only

To disable distributed forwarding on a distributed platform, use the **ipv6 mfib-mode centralized-only** command in global configuration mode. To reenable multicast forwarding, use the **no** form of this command.

ipv6 mfib-mode centralized-only

no ipv6 mfib-mode centralized-only

Syntax Description

This command has no arguments or keywords.

Command Default

Multicast distributed forwarding is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.3(4)T	This command was 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.

Usage Guidelines

Distributed forwarding is enabled by default when the **ipv6 multicast-routing**, **ipv6 cef distributed**, and the **ipv6 mfib** commands are enabled. The **ipv6 mfib-mode centralized-only** command disables distributed forwarding. All multicast forwarding is performed centrally.

Examples

The following example reenables distributed forwarding:

```
ipv6 mfib-mode centralized-only
```

ipv6 mld access-group

To perform IPv6 multicast receiver access control, use the **ipv6 mld access-group** command in interface configuration mode. To stop using multicast receiver access control, use the **no** form of this command.

ipv6 mld access-group *access-list-name*

no ipv6 mld access-group *access-list-name*

Syntax Description

access-list-name	A standard IPv6 named access list that defines the multicast groups and sources to allow or deny.

Command Default

All groups and sources are allowed.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
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.
12.2(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 **ipv6 mld access-group** command is used for receiver access control and to check the groups and sources in Multicast Listener Discovery (MLD) reports against the access list. The **ipv6 mld access-group** command also limits the state created by MLD reports. Because Cisco supports MLD version 2, the **ipv6 mld access-group** command allows users to limit the list of groups a receiver can join. You can also use this command to allow or deny sources used to join Source Specific Multicast (SSM) channels.

If a report (S1, S2...Sn, G) is received, the group (0, G) is first checked against the access list. If the group is denied, the entire report is denied. If the report is allowed, each individual (Si, G) is checked against the access list. State is not created for the denied sources.

Examples

The following example creates an access list called acc-grp-1 and denies all the state for group ff04::10:

```
Router(config)# ipv6 access-list acc-grp-1
Router(config-ipv6-acl)# deny ipv6 any host ff04::10
Router(config-ipv6-acl)# permit ipv6 any any
```

```
Router(config-ipv6-acl)# interface ethernet 0/0
Router(config-if)# ipv6 mld access-group acc-grp-1
```

The following example creates an access list called acc-grp-1 and permits all the state for only group ff04::10:

```
Router(config)# ipv6 access-list acc-grp-1
Router(config-ipv6-acl)# permit ipv6 any host ff04::10
Router(config-ipv6-acl)# interface ethernet 0/0
Router(config-if)# ipv6 mld access-group acc-grp-1
```

The following example permits only EXCLUDE(G,{}) reports. This example converts EXCLUDE(G,{S1, S2..Sn}) into EXCLUDE(G,{}):

```
Router(config)# ipv6 access-list acc-grp-1
Router(config-ipv6-acl)# permit ipv6 host :: host ff04::10
Router(config-ipv6-acl)# deny ipv6 any host ff04::10
Router(config-ipv6-acl)# permit ipv6 any any
Router(config-ipv6-acl)# interface ethernet 0/0
Router(config-if)# ipv6 mld access-group acc-grp-1
```

The following example filters a particular source 100::1 for a group ff04::10:

```
Router(config)# ipv6 access-list acc-grp-1
Router(config-ipv6-acl)# deny ipv6 host 100::1 host ff04::10
Router(config-ipv6-acl)# permit ipv6 any host ff04::10
Router(config-ipv6-acl)# interface ethernet 0/0
Router(config-if)# ipv6 mld access-group acc-grp-1
```

ipv6 mld explicit-tracking

To enable explicit tracking of hosts, use the **ipv6 mld explicit-tracking** command in interface configuration mode. To disable this function, use the **no** form of this command.

ipv6 mld explicit-tracking *access-list-name*

no ipv6 mld explicit-tracking *access-list-name*

Syntax Description

access-list-name	A standard IPv6 named access list that defines the multicast groups and sources to allow or deny.

Command Default

Explicit tracking is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
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.
12.2(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

When explicit tracking is enabled, the fast leave mechanism can be used with Multicast Listener Discovery (MLD) version 2 host reports. The *access-list-name* argument specifies a named IPv6 access list that can be used to specify the group ranges for which a user wants to apply explicit tracking.

Examples

The following example shows how to enable MLD explicit tracking on an access list named list1:

```
ipv6 mld explicit-tracking list1
```

ipv6 mld host-proxy

To enable the Multicast Listener Discovery (MLD) proxy feature, use the **ipv6 mld host-proxy** command in global configuration mode. To disable support for this feature, use the **no** form of this command.

ipv6 mld host-proxy [*group-acl*]

no ipv6 mld host-proxy

Syntax Description

group-acl	(Optional) Group access list (ACL).

Command Default

The MLD proxy feature is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

Use the **ipv6 mld host-proxy** command to enable the MLD proxy feature. If the *group-acl* argument is specified, the MLD proxy feature is supported for the multicast route entries that are permitted by the group ACL. If the *group-acl* argument is not provided, the MLD proxy feature is supported for all multicast routes present in multicast routing table.

Only one group ACL is configured at a time. Users can modify the group ACL by entering this command using a different *group-acl* argument.

Examples

The following example enables the MLD proxy feature for the multicast route entries permitted by the group ACL named “proxy-group”:

```
Router(config)# ipv6 mld host-proxy proxy-group
```

Related Commands

Command	Description
ipv6 mld host-proxy interface	Enables the MLD proxy feature on a specified interface on an RP.
show ipv6 mld host-proxy	Displays IPv6 MLD host proxy information.

ipv6 mld host-proxy interface

To enable the Multicast Listener Discovery (MLD) proxy feature on a specified interface on a Route Processor (RP), use the **ipv6 mld host-proxy interface** command in global configuration mode. To disable the MLD proxy feature on a RP, use the **no** form of this command.

ipv6 mld host-proxy interface [*group-acl*]

no ipv6 mld host-proxy interface

Syntax Description

group-acl	(Optional) Group access list (ACL).

Command Default

The MLD proxy feature is not enabled on the RP.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

Use the **ipv6 mld host-proxy interface** command to enable the MLD proxy feature on a specified interface on an RP. If a router is acting as an RP for an multicast-route proxy entry, it generates an MLD report on the specified host-proxy interface. Only one interface can be configured as a host-proxy interface, and the host-proxy interface can be modified by using this command with a different interface name.

If a router is not acting as an RP, enabling this command does not have any effect, nor will it generate an error or warning message.

Examples

The following example specifies Ethernet 0/0 as the host-proxy interface:

```
Router (config)# ipv6 mld host-proxy interface Ethernet 0/0
```

Related Commands

Command	Description
ipv6 mld host-proxy	Enables the MLD proxy feature.
show ipv6 mld host-proxy	Displays IPv6 MLD host proxy information.

ipv6 mld join-group

To configure Multicast Listener Discovery (MLD) reporting for a specified group and source, use the **ipv6 mld join-group** command in interface configuration mode. To cancel reporting and leave the group, use the **no** form of this command.

ipv6 mld join-group [*group-address*] [[**include** | **exclude**] {*source-address* | **source-list** [*acl*]}

no ipv6 mld join-group [*group-address*] [[**include** | **exclude**] {*source-address* | **source-list** [*acl*]}

Syntax Description

group-address	(Optional) IPv6 address of the multicast group.
include	(Optional) Enables include mode.
exclude	(Optional) Enables exclude mode.
source-address	Unicast source address to include or exclude.
source-list	Source list on which MLD reporting is to be configured.
acl	(Optional) Access list used to include or exclude multiple sources for the same group.

Command Default

If a source is specified and no mode is specified, the default is to include the source.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
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.
12.2(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 **ipv6 mld join-group** command configures MLD reporting for a specified source and group. The packets that are addressed to a specified group address will be passed up to the client process in the router. The packets will be forwarded out the interface depending on the normal Protocol Independent Multicast (PIM) activity.

The **source-list** keyword and *acl* argument may be used to include or exclude multiple sources for the same group. Each source is included in the access list in the following format:

permit ipv6 host *source* **any**

If the **ipv6 mld join-group** command is repeated for the same group, only the most recent command will take effect. For example, if you enter the following commands, only the second command is saved and will appear in the MLD cache:

```
Router(config-if)# ipv6 mld join-group ff05::10 include 2000::1
Router(config-if)# ipv6 mld join-group ff05::10 include 2000::2
```

Examples

The following example configures MLD reporting for specific groups:

```
Router(config-if)# ipv6 mld join-group ff04::10
```

Related Commands

Command	Description
no ipv6 mld router	Disables MLD router-side processing on a specified interface.

ipv6 mld limit

To limit the number of Multicast Listener Discovery (MLD) states on a per-interface basis, use the **ipv6 mld limit** command in interface configuration mode. To disable a configured MLD state limit, use the **no** form of this command.

ipv6 mld limit *number* [**except** *access-list*]

no ipv6 mld limit *number* [**except** *access-list*]

Syntax Description

number	Maximum number of MLD states allowed on a router. The valid range is from 1 to 64000.
except	(Optional) Excludes an access list from the configured MLD state limit.
access-list	(Optional) Access list to exclude from the configured MLD state limit.

Command Default

No default number of MLD limits is configured. You must configure the number of maximum MLD states allowed per interface on a router when you configure this command.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(50)SY	This command was modified. It was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

Use the **ipv6 mld limit** command to configure a limit on the number of MLD states resulting from MLD membership reports on a per-interface basis. Membership reports sent after the configured limits have been exceeded are not entered in the MLD cache, and traffic for the excess membership reports is not forwarded.

Use the **ipv6 mld state-limit** command in global configuration mode to configure the global MLD state limit.

Per-interface and per-system limits operate independently of each other and can enforce different configured limits. A membership state will be ignored if it exceeds either the per-interface limit or global limit.

If you do not configure the **except** *access-list* keyword and argument, all MLD states are counted toward the configured cache limit on an interface. Use the **except** *access-list* keyword and argument to exclude particular groups or channels from counting toward the MLD cache limit. An MLD membership report is counted against the per-interface limit if it is permitted by the extended access list specified by the **except** *access-list* keyword and argument.

Examples

The following example shows how to limit the number of MLD membership reports on Ethernet interface 0:

```
interface ethernet 0
 ipv6 mld limit 100
```

The following example shows how to limit the number of MLD membership reports on Ethernet interface 0. In this example, any MLD membership reports from access list cisco1 do not count toward the configured state limit:

```
interface ethernet 0
 ipv6 mld limit 100 except cisco1
```

Related Commands

Command	Description
ipv6 mld access-group	Enables the user to perform IPv6 multicast receiver access control.
ipv6 mld state-limit	Limits the number of MLD states on a global basis.

ipv6 mld query-interval

To configure the frequency at which the Cisco IOS software sends Multicast Listener Discovery (MLD) host-query messages, use the **ipv6 mld query-interval** command in interface configuration mode. To return to the default frequency, use the **no** form of this command.

ipv6 mld query-interval *seconds*

no ipv6 mld query-interval

Syntax Description

seconds	Frequency, in seconds, at which to send MLD host-query messages. It can be a number from 0 to 65535. The default is 125 seconds.

Command Default

The default is 125 seconds.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
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.
12.2(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

Multicast routers send host membership query messages (host-query messages) to discover which multicast groups have members on the router's attached networks. Hosts respond with MLD report messages indicating that they want to receive multicast packets for specific groups (that is, indicating that the host wants to become a member of the group).

The designated router for a LAN is the only router that sends MLD host-query messages.

The query interval is calculated as query timeout = (2 x query interval) + query-max-response-time / 2. If the **ipv6 mld query-interval** command is configured to be 60 seconds and the **ipv6 mld query-max-response-time** command is configured to be 20 seconds, then the **ipv6 mld command** should be configured to be 130 seconds or higher.

This command works with the **ipv6 mld query-max-response-time** and **ipv6 mld** commands. If you change the default value for the **ipv6 mld query-interval** command, make sure the changed value works correctly with these two commands.

Caution Changing the default value may severely impact multicast forwarding.

Examples

The following example sets the MLD query interval to 60 seconds:

```
Router(config)# interface FastEthernet 1/0
Router(config-if)# ipv6 mld query-interval 60
```

Related Commands

Command	Description
ipv6 mld query-max-response-time	Configures the maximum response time advertised in MLD queries.
ipv6 mld	Configures the timeout value before the router takes over as the querier for the interface.
ipv6 pim hello-interval	Configures the frequency of PIM hello messages on an interface.
show ipv6 mld groups	Displays the multicast groups that are directly connected to the router and that were learned through MLD.

ipv6 mld query-max-response-time

To configure the maximum response time advertised in Multicast Listener Discovery (MLD) queries, use the **ipv6 mld query-max-response-time** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ipv6 mld query-max-response-time *seconds*

no ipv6 mld query-max-response-time

Syntax Description

seconds	Maximum response time, in seconds, advertised in MLD queries. The default value is 10 seconds.

Command Default

The default is 10 seconds.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
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.
12.2(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

This command controls how much time the hosts have to answer an MLD query message before the router deletes their group. Configuring a value of fewer than 10 seconds enables the router to prune groups faster.

Note If the hosts do not respond fast enough, they might be pruned inadvertently. Therefore, the hosts must know to respond faster than 10 seconds (or the value you configure).

The query interval is calculated as query timeout = (2 x query interval) + query-max-response-time / 2. If the **ipv6 mld query-interval** command is configured to be 60 seconds and the **ipv6 mld query-max-response-time** command is configured to be 20 seconds, then the **ipv6 mld command** should be configured to be 130 seconds or higher.

This command works with the **ipv6 mld query-interval** and **ipv6 mld** commands. If you change the default value for the **ipv6 mld query-max-response-time** command, make sure the changed value works correctly with these two commands.

Caution Changing the default value may severely impact multicast forwarding.

Examples

The following example configures a maximum response time of 20 seconds:

```
Router(config)# interface FastEthernet 1/0
Router(config-if)# ipv6 mld query-max-response-time 20
```

Related Commands

Command	Description
ipv6 mld query-interval	Configures the frequency at which the Cisco IOS software sends MLD host-query messages.
ipv6 mld	Configures the timeout value before the router takes over as the querier for the interface.
ipv6 pim hello-interval	Configures the frequency of PIM hello messages on an interface.
show ipv6 mld groups	Displays the multicast groups that are directly connected to the router and that were learned through MLD.

ipv6 mld query-timeout

To configure the timeout value before the router takes over as the querier for the interface, use the **ipv6 mld query-timeout** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ipv6 mld query-timeout *seconds*

no ipv6 mld query-timeout

Syntax Description

seconds	Number of seconds that the router waits after the previous querier has stopped querying and before it takes over as the querier.

Command Default

The default is 255 seconds.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
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.
12.2(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 query interval is calculated as query timeout = (2 x query interval) + query-max-response-time / 2. If the **ipv6 mld query-interval** command is configured to be 60 seconds and the **ipv6 mld query-max-response-time** command is configured to be 20 seconds, then the **ipv6 mld query-timeout command** should be configured to be 130 seconds or higher.

This command works with the **ipv6 mld query-interval** and **ipv6 mld query-max-response-time** commands. If you change the default value for the **ipv6 mld query-timeout** command, make sure the changed value works correctly with these two commands.

Caution Changing the default value may severely impact multicast forwarding.

Examples

The following example configures the router to wait 130 seconds from the time it received the last query before it takes over as the querier for the interface:

```
Router(config)# interface FastEthernet 1/0
Router(config-if)# ipv6 mld query-timeout 130
```

Related Commands

Command	Description
ipv6 mld query-interval	Configures the frequency at which the Cisco IOS software sends MLD host-query messages.
ipv6 mld query-max-response-time	Configures the maximum response time advertised in MLD queries.

ipv6 mld router

To enable Multicast Listener Discovery (MLD) group membership message processing and routing on a specified interface, use the **ipv6 mld router** command in interface configuration mode. To disable MLD group membership message processing and routing on a specified interface, use the **no** form of the command.

ipv6 mld router

no ipv6 mld router

Syntax Description

This command has no arguments or keywords.

Command Default

MLD message processing and egress routing of multicast packets is enabled on the interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
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.
12.2(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

When the **ipv6 multicast-routing** command is configured, MLD group membership message processing is enabled on every interface. The **no ipv6 mld router** command prevents forwarding (routing) of multicast packets to the specified interface and disables static multicast group configuration on the specified interface.

The **no ipv6 mld router** command also disables MLD group membership message processing on a specified interface. When MLD group membership message processing is disabled, the router stops sending MLD queries and stops keeping track of MLD members on the LAN.

If the **ipv6 mld join-group** command is also configured on an interface, it will continue with MLD host functionality and will report group membership when an MLD query is received.

MLD group membership processing is enabled by default. The **ipv6 multicast-routing** command does not enable or disable MLD group membership message processing.

Examples

The following example disables MLD group membership message processing on an interface and disables routing of multicast packets to that interface:

```
Router(config)# interface FastEthernet 1/0
Router(config-if)# no ipv6 mld router
```

Related Commands

Command	Description
ipv6 mld join-group	Configures MLD reporting for a specified group and source.
ipv6 multicast-routing	Enables multicast routing using PIM and MLD on all IPv6-enabled interfaces of the router and enables multicast forwarding.

ipv6 mld snooping

To enable Multicast Listener Discovery version 2 (MLDv2) protocol snooping globally, use the **ipv6 mld snooping** command in global configuration mode. To disable the MLDv2 snooping globally, use the **no** form of this command.

ipv6 mld snooping

no ipv6 mld snooping

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	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

MLDv2 snooping is supported on the Supervisor Engine 720 with all versions of the Policy Feature Card 3 (PFC3).

To use MLDv2 snooping, configure a Layer 3 interface in the subnet for IPv6 multicast routing or enable the MLDv2 snooping querier in the subnet.

Examples

This example shows how to enable MLDv2 snooping globally:

```
Router(config)# ipv6 mld snooping
```

Related Commands

Command	Description
show ipv6 mld snooping	Displays MLDv2 snooping information.

ipv6 mld snooping explicit-tracking

To enable explicit host tracking, use the **ipv6 mld snooping explicit-tracking** command in interface configuration mode. To disable explicit host tracking, use the **no** form of this command.

ipv6 mld snooping explicit-tracking

no ipv6 mld snooping explicit-tracking

Syntax Description

This command has no arguments or keywords.

Command Default

Explicit host tracking is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(18)SXE	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.

Explicit host tracking is supported only with Internet Group Management Protocol Version 3 (IGMPv3) hosts.

When you enable explicit host tracking and the Cisco 7600 series router is working in proxy-reporting mode, the router may not be able to track all the hosts that are behind a VLAN interface. In proxy-reporting mode, the Cisco 7600 series router forwards only the first report for a channel to the router and suppresses all other reports for the same channel.

With IGMPv3 proxy reporting, the Cisco 7600 series router does proxy reporting for unsolicited reports and reports that are received in the general query interval.

Proxy reporting is turned on by default. When you disable proxy reporting, the Cisco 7600 series router works in transparent mode and updates the IGMP snooping database as it receives reports and forwards this information to the upstream router. The router can then explicitly track all reporting hosts.

Disabling explicit tracking disables fast-leave processing and proxy reporting.

IGMPv3 supports explicit host tracking of membership information on any port. The explicit host-tracking database is used for fast-leave processing for IGMPv3 hosts, proxy reporting, and statistics collection. When you enable explicit host tracking on a VLAN, the IGMP snooping software processes the IGMPv3 report that it receives from a host and builds an explicit host-tracking database that contains the following information:

- The port that is connected to the host.
- The channels that are reported by the host.
- The filter mode for each group that are reported by the host.

- The list of sources for each group that are reported by the hosts.
- The router filter mode of each group.
- The list of hosts for each group that request the source.

Examples

This example shows how to enable explicit host tracking:

```
Router(config-if)# ipv6 mld snooping explicit-tracking
```

Related Commands

Command	Description
ipv6 mld snooping limit	Configures the MLDv2 limits.
show ipv6 mld snooping	Displays MLDv2 snooping information.

ipv6 mld snooping last-member-query-interval

To configure the last member query interval for Multicast Listener Discovery Version 2 (MLDv2) snooping, use the **ipv6 mld snooping last-member-query-interval** command in interface configuration. To return to the default settings, use the **no** form of this command.

ipv6 mld snooping last-member-query-interval *interval*

no ipv6 mld snooping last-member-query-interval

Syntax Description

interval	Interval for the last member query; valid values are from 100 to 900 milliseconds in multiples of 100 milliseconds.

Command Default

The default is 1000 milliseconds (1 second).

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	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 12.2(33)SRA.

Usage Guidelines

When a multicast host leaves a group, the host sends an IGMP leave. To check if this host is the last to leave the group, an IGMP query is sent out when the leave is seen and a timer is started. If no reports are received before the timer expires, the group record is deleted.

The *interval* is the actual time that the Cisco 7600 series router waits for a response for the group-specific query.

If you enter an interval that is not a multiple of 100, the interval is rounded to the next lowest multiple of 100. For example, if you enter 999, the interval is rounded down to 900 milliseconds.

If you enable IGMP fast-leave processing and you enter the **no ipv6 mld snooping last-member-query-interval** command, the interval is set to 0 seconds; fast-leave processing always assumes a higher priority.

Even though the valid interval range is 100 to 1000 milliseconds, you cannot enter a value of **1000**. If you want this value, you must enter the **no ipv6 mld snooping last-member-query-interval** command and return to the default value (1000 milliseconds).

Examples

This example shows how to configure the last member query interval to 200 milliseconds:

```
Router(config-if)# ipv6 mld snooping last-member-query-interval 200
Router(config-if)#
```

Related Commands

Command	Description
show ipv6 mld snooping	Displays MLDv2 snooping information.

ipv6 mld snooping limit

To configure Multicast Listener Discovery version 2 (MLDv2) protocol limits, use the **ipv6 mld snooping limit** command in global configuration mode. To return to the default settings, use the **no** form of this command.

ipv6 mld snooping limit {**l2-entry-limit** *max-entries* | **rate** *pps* | **track** *max-entries*}

no ipv6 mld snooping limit {**l2-entry-limit** | **rate** | **track**}

Syntax Description

l2-entry-limit *max-entries*	Specifies the maximum number of Layer 2 entries that can be installed by MLD snooping. Valid values are from 1 to 100000 entries.
rate *pps*	Specifies the rate limit of incoming MLDv2 messages. Valid values are from 100 to 6000 packets per second (pps).
track *max-entries*	Specifies the maximum number of entries in the explicit-tracking database. Valid values are from 0 to 128000 entries.

Command Default

The *max-entries* argument default is 32000.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	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.

Each entry in the explicit-tracking database is identified by the source IP, group IP, port, VLAN, and reporter IP.

When you set the *max-entries* argument to 0, explicit-tracking is disabled.

When the explicit-tracking database exceeds the configured *max-entries* value, a system logging message is generated.

When you reduce the *max-entries* argument, the explicit-tracking database does not decrease in size immediately. The explicit-tracking database gradually shrinks as reporters time out.

Examples

This example shows how to set the maximum number of Layer 2 entries that can be installed by MLD snooping:

```
Router(config)# ipv6 mld snooping limit l2-entry-limit 100000
```

This example shows how to set the rate limit for incoming MLDv2-snooping packets:

```
Router(config)# ipv6 mld snooping limit rate 200
```

This example shows how to configure the maximum number of entries in the explicit-tracking database:

```
Router(config)# ipv6 mld snooping limit track 20000
```

This example shows how to disable software rate limiting:

```
Router(config)# no ipv6 mld snooping limit rate
```

Related Commands

Command	Description
ipv6 mld snooping explicit tracking	Enables explicit host tracking.

ipv6 mld snooping mrouter

To configure a Layer 2 port as a multicast router port, use the **ipv6 mld snooping mrouter** command in interface configuration mode.

ipv6 mld snooping mrouter interface *type slot/port*

Syntax Description

interface *type*	Specifies the interface type: valid values are **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**.
slot/port	Module and port number. The slash mark is required.

Command Default

No defaults are configured.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(18)SXE	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.

Examples

This example shows how to configure a Layer 2 port as a multicast router port:

```
Router(config-if)# ipv6 mld snooping mrouter interface fastethernet 5/6
```

Related Commands

Command	Description
mac-address-table static	Adds static entries to the MAC address table.
show ipv6 mld snooping	Displays MLDv2 snooping information.

ipv6 mld snooping querier

To enable the Multicast Listener Discovery version 2 (MLDv2) snooping querier, use the **ipv6 mld snooping querier** command in interface configuration mode. To disable the MLDv2 snooping querier, use the **no** form of this command.

ipv6 mld snooping querier

no ipv6 mld snooping querier

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(18)SXE	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

You must configure an IPv6 address on the VLAN interface. When this feature is enabled, the MLDv2 snooping querier uses the IPv6 address as the query source address.

If there is no IPv6 address configured on the VLAN interface, the MLDv2 snooping querier does not start. The MLDv2 snooping querier disables itself if the IPv6 address is cleared. When this feature is enabled, the MLDv2 snooping querier restarts if you configure an IPv6 address.

The MLDv2 snooping querier:

- Does not start if it detects MLDv2 traffic from an IPv6 multicast router.
- Starts after 60 seconds if it detects no MLDv2 traffic from an IPv6 multicast router.
- Disables itself if it detects MLDv2 traffic from an IPv6 multicast router.

You can enable the MLDv2 snooping querier on all the Catalyst 6500 series switches in the VLAN that support it. One switch is elected as the querier.

Examples

This example shows how to enable the MLDv2 snooping querier on VLAN 200:

```
Router(config)# interface vlan 200
Router(config-if)# ipv6 mld snooping querier
```

Related Commands

Command	Description
show ipv6 mld snooping	Displays MLDv2 snooping information.

ipv6 mld snooping report-suppression

To enable Multicast Listener Discovery version 2 (MLDv2) report suppression on a VLAN, use the **ipv6 mld snooping report-suppression** command in interface configuration mode. To disable report suppression on a VLAN, use the **no** form of this command.

ipv6 mld snooping report-suppression

no ipv6 mld snooping report-suppression

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(18)SXE	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

You must enable explicit tracking before enabling report suppression.

This command is supported on VLAN interfaces only.

Examples

This example shows how to enable explicit host tracking:

```
Router(config-if)# ipv6 mld snooping report-suppression
```

ipv6 mld ssm-map enable

To enable the Source Specific Multicast (SSM) mapping feature for groups in the configured SSM range, use the **ipv6 mld ssm-map enable** command in global configuration mode. To disable this feature, use the **no** form of this command.

ipv6 mld [**vrf** *vrf-name*] **ssm-map enable**

no ipv6 mld [**vrf** *vrf-name*] **ssm-map enable**

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Default

The SSM mapping feature is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	This command was introduced.
12.4(2)T	This command was integrated into Cisco IOS Release 12.4(2)T.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

The **ipv6 mld ssm-map enable** command enables the SSM mapping feature for groups in the configured SSM range. When the **ipv6 mld ssm-map enable** command is used, SSM mapping defaults to use the Domain Name System (DNS).

SSM mapping is applied only to received Multicast Listener Discovery (MLD) version 1 or MLD version 2 membership reports.

Examples

The following example shows how to enable the SSM mapping feature:

```
Router(config)# ipv6 mld ssm-map enable
```

Related Commands

Command	Description
debug ipv6 mld ssm-map	Displays debug messages for SSM mapping.
ipv6 mld ssm-map query dns	Enables DNS-based SSM mapping.

Command	Description
ipv6 mld ssm-map static	Configures static SSM mappings.
show ipv6 mld ssm-map	Displays SSM mapping information.

ipv6 mld ssm-map query dns

To enable Domain Name System (DNS)-based Source Specific Multicast (SSM) mapping, use the **ipv6 mld ssm-map query dns** command in global configuration mode. To disable DNS-based SSM mapping, use the **no** form of this command.

ipv6 mld [**vrf** *vrf-name*] **ssm-map query dns**

no ipv6 mld [**vrf** *vrf-name*] **ssm-map query dns**

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Default

DNS-based SSM mapping is enabled by default when the SSM mapping feature is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	This command was introduced.
12.4(2)T	This command was integrated into Cisco IOS Release 12.4(2)T.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

DNS-based SSM mapping is enabled by default when the SSM mapping feature is enabled using the **ipv6 mld ssm-map enable** command. If DNS-based SSM mapping is disabled by entering the **no** version of the **ipv6 mld ssm-map query dns** command, only statically mapped SSM sources configured by the **ipv6 mld ssm-map static** command will be determined.

For DNS-based SSM mapping to succeed, the router needs to find at least one correctly configured DNS server.

Examples

The following example enables the DNS-based SSM mapping feature:

```
ipv6 mld ssm-map query dns
```

Related Commands

Command	Description
debug ipv6 mld ssm-map	Displays debug messages for SSM mapping.
ipv6 mld ssm-map enable	Enables the SSM mapping feature for groups in the configured SSM range.
ipv6 mld ssm-map static	Configures static SSM mappings.
show ipv6 mld ssm-map	Displays SSM mapping information.

ipv6 mld ssm-map static

To configure static Source Specific Multicast (SSM) mappings, use the **ipv6 mld ssm-map static** command in global configuration mode. To disable this feature, use the **no** form of this command.

ipv6 mld [**vrf** *vrf-name*] **ssm-map static** *access-list source-address*

no ipv6 mld [**vrf** *vrf-name*] **ssm-map static** *access-list source-address*

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
access-list	Name of the IPv6 access list that identifies a group range. Access list names cannot contain a space or quotation mark, or begin with a numeric.
source-address	Source address associated with an MLD membership for a group identified by the access list.

Command Default

The SSM mapping feature is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	This command was introduced.
12.4(2)T	This command was integrated into Cisco IOS Release 12.4(2)T.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

Use the **ipv6 mld ssm-map static** command to configure static SSM mappings. If SSM mapping is enabled and the router receives a Multicast Listener Discovery (MLD) membership for group G in the SSM range, the router tries to determine the source addresses associated with G by checking the **ipv6 mld ssm-map static** command configurations.

If group G is permitted by the access list identified by the *access-list* argument, then the specified source address is used. If multiple static SSM mappings have been configured using the **ipv6 mld ssm-map static** command and G is permitted by multiple access lists, then the source addresses of all matching access lists will be used (the limit is 20).

If no static SSM mappings in the specified access lists match the MLD membership, SSM mapping queries the Domain Name System (DNS) for address mapping.

Examples

The following example enables the SSM mapping feature and configures the groups identified in the access list named SSM_MAP_ACL_2 to use source addresses 2001:0DB8:1::1 and 2001:0DB8:1::3:

```
ipv6 mld ssm-map enable
ipv6 mld ssm-map static SSM_MAP_ACL_2 2001:0DB8:1::1
ipv6 mld ssm-map static SSM_MAP_ACL_2 2001:0DB8:1::3
ipv6 mld ssm-map query dns
```

Related Commands

Command	Description
debug ipv6 mld ssm-map	Displays debug messages for SSM mapping.
ipv6 mld ssm-map enable	Enables the SSM mapping feature for groups in the configured SSM range.
ipv6 mld ssm-map query dns	Enables DNS-based SSM mapping.
show ipv6 mld ssm-map	Displays SSM mapping information.

ipv6 mld state-limit

To limit the number of Multicast Listener Discovery (MLD) states globally, use the **ipv6 mld state-limit** command in global configuration mode. To disable a configured MLD state limit, use the **no** form of this command.

ipv6 mld state-limit *number*

no ipv6 mld state-limit *number*

Syntax Description

number	Maximum number of MLD states allowed on a router. The valid range is from 1 to 64000.

Command Default

No default number of MLD limits is configured. You must configure the number of maximum MLD states allowed globally on a router when you configure this command.

Command Modes

Global configuration

Command History

Release	Modification
12.4(2)T	This command was introduced.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(50)SY	This command was modified. It was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

Use the **ipv6 mld state-limit** command to configure a limit on the number of MLD states resulting from MLD membership reports on a global basis. Membership reports sent after the configured limits have been exceeded are not entered in the MLD cache and traffic for the excess membership reports is not forwarded.

Use the **ipv6 mld limit** command in interface configuration mode to configure the per-interface MLD state limit.

Per-interface and per-system limits operate independently of each other and can enforce different configured limits. A membership state will be ignored if it exceeds either the per-interface limit or global limit.

Examples

The following example shows how to limit the number of MLD states on a router to 300:

```
ipv6 mld state-limit 300
```

Related Commands

Command	Description
ipv6 mld access-group	Enables the performance of IPv6 multicast receiver access control.
ipv6 mld limit	Limits the number of MLD states resulting from MLD membership state on a per-interface basis.

ipv6 mld static-group

To statically forward traffic for the multicast group onto a specified interface and cause the interface to behave as if a Multicast Listener Discovery (MLD) joiner were present on the interface, use the **ipv6 mld static-group** command in interface configuration mode. To stop statically forwarding traffic for the specific multicast group, use the **no** form of this command.

ipv6 mld static-group [*group-address*] [[**include** | **exclude**] {*source-address* | **source-list** [*acl*]}

no ipv6 mld static-group [*group-address*] [[**include** | **exclude**] {*source-address* | **source-list** [*acl*]}

Syntax Description

group-address	(Optional) IPv6 address of the multicast group.
include	(Optional) Enables include mode.
exclude	(Optional) Enables exclude mode.
source-address	Unicast source address to include or exclude.
source-list	Source list on which MLD reporting is to be configured.
acl	(Optional) Access list used to include or exclude multiple sources for the same group.

Command Default

If no mode is specified for the source, use of the **include** keyword is the default.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
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.
12.2(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 **ipv6 multicast-routing** command must be configured for the **ipv6 mld static-group** command to be effective.

When the **ipv6 mld static-group** command is enabled, packets to the group are either fast-switched or hardware-switched, depending on the platform. Unlike what happens when using the **ipv6 mld join-group** command, a copy of the packet is not sent to the process level.

An access list can be specified to include or exclude multiple sources for the same group. Each source is included in the access list in the following format:

permit ipv6 host *source* **any**

Note Using the **ipv6 mld static-group** command is not sufficient to allow traffic to be forwarded onto the interface. Other conditions, such as the absence of a route, the router not being the designated router, or losing an assert, can cause the router not to forward traffic even if the **ipv6 mld static-group** command is configured.

Examples

The following example statically forward traffic for the multicast group onto the specified interface:

```
ipv6 mld static-group ff04::10 include 100::1
```

Related Commands

Command	Description
ipv6 mld join-group	Configures MLD reporting for a specified group and source.
no ipv6 mld router	Disables MLD router-side processing on a specified interface.
ipv6 multicast-routing	Enables multicast routing using PIM and MLD on all IPv6-enabled interfaces of the router and enables multicast forwarding.
no ipv6 pim	Use the **no** form of the **ipv6 pim** command to disable PIM on a specified interface.

ipv6 mobile home-agent (global configuration)

To enter home agent configuration mode, use the **ipv6 mobile home-agent** command in global configuration mode. To reset to the default settings of the command, use the **no** form of this command.

ipv6 mobile home-agent

no ipv6 mobile home-agent

Syntax Description

This command has no arguments or keywords.

Command Default

Mobile IPv6 home agent is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

Use the **ipv6 mobile home-agent** command to enter home agent configuration mode. Once in home agent configuration mode, you can configure binding parameters using the **binding** command. Once an interface is configured to provide the home-agent service, the **ipv6 mobile home-agent** global configuration command automatically appears in the global configuration.

The home agent service needs to be started on each interface using the **ipv6 mobile home-agent** command in interface configuration mode. The **ipv6 mobile home-agent** command in global configuration mode does not start home agent service on an interface.

Examples

In the following example, the user enters home agent configuration mode:

```
Router(config)# ipv6 mobile home-agent
Router(config-ha)#
```

Related Commands

Command	Description
binding	Configures binding options for the Mobile IPv6 home agent feature in home agent configuration mode.
ipv6 mobile home-agent (interface configuration)	Initializes and starts the Mobile IPv6 home agent on a specific interface.
show ipv6 mobile globals	Displays global Mobile IPv6 parameters.

ipv6 mobile home-agent (interface configuration)

To initialize and start the Mobile IPv6 home agent on a specific interface, use the **ipv6 mobile home-agent** command in interface configuration mode. To discard bindings and any interface parameter settings, and to terminate home agent operation on a specific interface, use the **no** form of this command.

ipv6 mobile home-agent [**preference** *preference-value*]

no ipv6 mobile home-agent

Syntax Description

preference *preference-value*	(Optional) Configures the Mobile IPv6 home agent preference value on a specified interface. The *preference-value* argument is an integer to be configured for preference in the home agent information option. The range is from 0 to 65535. The default preference value is 0.

Command Default

Mobile IPv6 home agent is disabled.
The default preference value is 0.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

Before you enable the **ipv6 mobile home-agent** (interface configuration) command on an interface, you should configure common parameters using the **binding** command. Once an interface is configured to run the home agent feature, the **ipv6 mobile home-agent** command in global configuration mode automatically appears in the global configuration.

Once enabled, the **ipv6 mobile home-agent** (interface configuration) command cannot be disabled if there is a home agent configured on at least one of the interfaces. If there is no home agent service on any interfaces, the **no** form of the command disables home agent capability from the router.

To configure the home agent preference value, use the optional **preference** *preference-value* keyword and argument. A preference value is a 16-bit signed integer used by the home agent sending a router advertisement. The preference value orders the addresses returned to the mobile node in the home agent addresses field of a home agent address discovery reply message. The higher the preference value, the more preferable is the home agent.

If a preference value is not included in a router advertisement, the default value is 0. Values greater than 0 indicate a home agent more preferable than this default value.

Examples

In the following example, the user initializes and starts Mobile IPv6 agent on Ethernet interface 2:

```
Router(config)# interface Ethernet 2
Router(config-if)# ipv6 mobile home-agent
```

In the following example, the home agent preference value is set to 10:

```
Router(config-if)# ipv6 mobile home-agent preference 10
```

Related Commands

Command	Description
binding	Configures binding options for the Mobile IPv6 home agent feature in home agent configuration mode.
ipv6 mobile home-agent (global configuration)	Enters home agent configuration mode.
show ipv6 mobile globals	Displays global Mobile IPv6 parameters.

ipv6 mobile router

To enable IPv6 network mobility (NEMO) functionality on a router and place the router in IPv6 mobile router configuration mode, use the **ipv6 mobile router** command in global configuration mode. To disable NEMO functionality on the router, use the **no** form of the command.

ipv6 mobile router

no ipv6 mobile router

Syntax Description

This command has no arguments or keywords.

Command Default

NEMO functionality is not enabled.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

The mobile router is a router that operates as a mobile node. The mobile router can roam from its home network and still provide connectivity for devices on its networks. The mobile networks are locally attached to the router.

Examples

In the following example, the mobile router is enabled:

```
Router(config)# ipv6 mobile router
```

ipv6 mobile router-service roam

To enable the IPv6 mobile router interface to roam, use the **ipv6 mobile router-service roam** command in interface configuration mode. To disable roaming, use the **no** form of this command.

ipv6 mobile router-service roam [**bandwidth-efficient | cost-efficient | priority** *value*]

no ipv6 mobile router-service roam

Syntax Description

bandwidth-efficient	(Optional) Enables the mobile router to use the largest configured lifetime value.
cost-efficient	(Optional) Prevents a binding update unless a dialup link is up and a valid care-of address is available.
priority *value*	(Optional) Priority value that is compared among multiple configured interfaces to select the interface in which to send the registration request. When multiple interfaces have highest priority, the highest bandwidth is the preferred choice. When multiple interfaces have the same bandwidth, the interface with the highest IPv6 address is preferred. The range is from 0 to 255; the default is 100. Lower values equate to a higher priority.

Command Default

Roaming is not enabled.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

The mobile router discovers home agents and foreign agents by receiving agent advertisements.

The **bandwidth-efficient** keyword enables the mobile router to use the largest configured lifetime value, even when the home agent recommends a shorter lifetime in a binding refresh advice message. This option can be used when the bandwidth is expensive.

Examples

The following example shows how to enable roaming for the IPv6 mobile router interface:

```
Router(config-if)# ipv6 mobile router-service roam
```

Related Commands

Command	Description
show ipv6 mobile router	Displays configuration information and monitoring statistics about the IPv6 mobile router.

ipv6 mtu

To set the maximum transmission unit (MTU) size of IPv6 packets sent on an interface, use the **ipv6 mtu** command in interface configuration mode. To restore the default MTU size, use the **no** form of this command.

ipv6 mtu *bytes*

no ipv6 mtu *bytes*

Syntax Description

bytes	MTU (in bytes).

Command Default

The default value depends on the interface medium, but the minimum for any interface is 1280 bytes.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)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 Release 12.2(14)S.
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.
12.2(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 a nondefault value is configured for an interface, an MTU option is included in router advertisements.

IPv6 routers do not fragment forwarded IPv6 packets. Traffic originating from IPv6 routers may be fragmented.

All devices on a physical medium must have the same protocol MTU in order to operate.

In addition to the "IPv6 MTU value" (set by using the **ipv6 mtu** command), interfaces also have a nonprotocol specific "MTU value," which is set by using the **mtu** interface configuration command.

Note The "MTU value" configured by using the **mtu** interface configuration command must not be less than 1280 bytes.

Examples

The following example sets the maximum IPv6 packet size for serial interface 0/1 to 2000 bytes:

```
Router(config)# interface serial 0/1
Router(config-if)# ipv6 mtu 2000
```

Related Commands

Command	Description
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 multicast aaa account receive

To enable authentication, authorization, and accounting (AAA) accounting on specified groups or channels, use the **ipv6 multicast aaa account receive** command in interface configuration mode. To disable AAA accounting, use the **no** form of this command.

ipv6 multicast aaa account receive *access-list-name* [**throttle** *throttle-number*]

no ipv6 multicast aaa account receive

Syntax Description

access-list-name	Access list to specify which groups or channels are to have AAA accounting enabled.
throttle	(Optional) Limits the number of records sent during channel surfing. No record is sent if a channel is viewed for less than a specified, configurable period of time.
throttle-number	(Optional) Throttle or surfing interval, in seconds.

Command Default

No AAA accounting is performed on any groups or channels.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

Note Including information about IPv6 addresses in accounting and authorization records transmitted between the router and the RADIUS or TACACS+ server is supported. However, there is no support for using IPv6 to communicate with that server. The server must have an IPv4 address.

Use the **ipv6 multicast aaa account receive** command to enable AAA accounting on specific groups or channels and to set throttle interval limits on records sent during channel surfing.

Examples

The following example enables AAA accounting using an access list named list1:

```
Router(config-if)# ipv6 multicast aaa account receive list1
```

Related Commands

Command	Description
aaa accounting multicast default	Enables AAA accounting of IPv6 multicast services for billing or security purposes when you use RADIUS.

ipv6 multicast boundary scope

To configure a multicast boundary on the interface for a specified scope, use the **ipv6 multicast boundary scope** command in interface configuration mode. To disable this feature, use the **no** form of this command.

ipv6 multicast boundary scope *scope-value*

no ipv6 multicast boundary scope *scope-value*

Syntax Description

scope-value	The scope value can be one of the following: • Link-local address • Subnet-local address • Admin-local address • Site-local address • Organization-local • Virtual Private Network (VPN) • Scope number, which is from 2 through 15

Command Default

Multicast boundary is not configured on the interface.

Command Modes

Interface 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.

Usage Guidelines

If the **ipv6 multicast boundary scope** command is configured for a particular scope on the Reverse Path Forwarding (RPF) interface, then packets are not accepted on that interface for groups that belong to scopes that are less than or equal to the one configured. Protocol Independent Multicast (PIM) join/prune messages for those groups are not sent on the RPF interface. The effect of the scope can be verified by checking the output of the **show ipv6 mrib route** command. The output will not show the RPF interface with Accept flag.

If the **ipv6 multicast boundary scope** command is configured for a particular scope on an interface in the outgoing interface list, packets are not forwarded for groups that belong to scopes that are less than or equal to the one configured.

Protocol Independent Multicast (PIM) join/prune (J/P) messages are not processed when received on the interface for groups that belong to scopes that are less than or equal to the one configured. Registers and bootstrap router (BSR) messages are also filtered on the boundary.

Examples

The following example sets the scope value to be a scope number of 6:

```
ipv6 multicast boundary scope 6
```

Related Commands

Command	Description
ipv6 pim bsr candidate bsr	Configures a router to be a candidate BSR.
ipv6 pim bsr candidate rp	Configures the candidate RP to send PIM RP advertisements to the BSR.
show ipv6 mrib route	Displays the MRIB route information.

ipv6 multicast group-range

To disable multicast protocol actions and traffic forwarding for unauthorized groups or channels on all the interfaces in a router, use the **ipv6 multicast group-range** command in global configuration mode. To return to the command's default settings, use the **no** form of this command.

ipv6 multicast [**vrf** *vrf-name*] **group-range** [*access-list-name*]

no ipv6 multicast [**vrf** *vrf-name*] **group-range** [*access-list-name*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
access-list-name	(Optional) Name of an access list that contains authenticated subscriber groups and authorized channels that can send traffic to the router.

Command Default

Multicast is enabled for groups and channels permitted by a specified access list and disabled for groups and channels denied by a specified access list.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(4)T	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 2.6	This command was introduced on Cisco ASR 1000 series routers.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

The **ipv6 multicast group-range** command provides an access control mechanism for IPv6 multicast edge routing. The access list specified by the *access-list-name* argument specifies the multicast groups or channels that are to be permitted or denied. For denied groups or channels, the router ignores protocol traffic and actions (for example, no Multicast Listener Discovery (MLD) states are created, no mroute states are created, no Protocol Independent Multicast (PIM) joins are forwarded), and drops data traffic on all interfaces in the system, thus disabling multicast for denied groups or channels.

Using the **ipv6 multicast group-range** global configuration command is equivalent to configuring the MLD access control and multicast boundary commands on all interfaces in the system. However, the **ipv6 multicast group-range** command can be overridden on selected interfaces by using the following interface configuration commands:

- **ipv6 mld access-group** *access-list-name*
- **ipv6 multicast boundary scope** *scope-value*

Because the **no ipv6 multicast group-range** command returns the router to its default configuration, existing multicast deployments are not broken.

Examples

The following example ensures that the router disables multicast for groups or channels denied by an access list named list2:

```
Router(config)# ipv6 multicast group-range list2
```

The following example shows that the command in the previous example is overridden on an interface specified by int2:

```
Router(config)# interface int2
Router(config-if)# ipv6 mld access-group int-list2
```

On int2, MLD states are created for groups or channels permitted by int-list2 but are not created for groups or channels denied by int-list2. On all other interfaces, the access-list named list2 is used for access control.

In this example, list2 can be specified to deny all or most multicast groups or channels, and int-list2 can be specified to permit authorized groups or channels only for interface int2.

Related Commands

Command	Description
ipv6 mld access-group	Performs IPv6 multicast receiver access control.
ipv6 multicast boundary scope	Configures a multicast boundary on the interface for a specified scope.

ipv6 multicast limit

To configure per-interface multicast route (mroute) state limiters in IPv6, use the **ipv6 multicast limit** command in interface configuration mode. To remove the limit imposed by a per-interface mroute state limiter, use the **no** form of this command.

ipv6 multicast limit [**connected** | **rpf** | **out**] *limit-acl max* [**threshold** *threshold-value*]

no ipv6 multicast limit [**connected** | **rpf** | **out**] *limit-acl max* [**threshold** *threshold-value*]

Syntax Description

connected	(Optional) Limits mroute states created for an Access Control List (ACL)-classified set of multicast traffic on an incoming (Reverse Path Forwarding [RPF]) interface that is directly connected to a multicast source by counting each time that an mroute permitted by the ACL is created or deleted.
rpf	(Optional) Limits the number of mroute states created for an ACL-classified set of multicast traffic on an incoming (RPF) interface by counting each time an mroute permitted by the ACL is created or deleted.
out	(Optional) Limits mroute outgoing interface list membership on an outgoing interface for an ACL-classified set of multicast traffic by counting each time that an mroute list member permitted by the ACL is added or removed.
limit-acl	Name identifying the ACL that defines the set of multicast traffic to be applied to a per-interface mroute state limiter.
max	Maximum number of mroutes permitted by the per interface mroute state limiter. The range is from 0 to 2147483647.
threshold	(Optional) The mCAC threshold percentage.
threshold-value	(Optional) The specified percentage. The threshold notification default is 0%, meaning that threshold notification is disabled.

Command Default

No per-interface mroute state limiters are configured.
Threshold notification is set to 0%; that is, it is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.
Cisco IOS XE Release 2.6	This command was introduced on Cisco ASR 1000 series routers.

Usage Guidelines

Use the **ipv6 multicast limit** command to configure mroute state limiters on an interface.

For the required *limit-acl* argument, specify the ACL that defines the IPv6 multicast traffic to be limited on an interface. A standard or extended ACL can be specified.

The **ipv6 multicast limit cost** command complements the per-interface **ipv6 multicast limit** command. Once the *limit-acl* argument is matched in the **ipv6 multicast limit** command, the *access-list* argument in the **ipv6 multicast limit cost** command is checked to see which cost to apply to limited groups. If no cost match is found, the default cost is 1.

The threshold notification for mCAC limit feature notifies the user when actual simultaneous multicast channel numbers exceeds or fall below a specified threshold percentage.

Examples

The following example configures the interface limit on the source router's outgoing interface Ethernet 1/3:

```
interface Ethernet1/3
ipv6 address FE80::40:1:3 link-local
 ipv6 address 2001:0DB8:1:1:3/64
 ipv6 multicast limit out acl1 10
```

Related Commands

Command	Description
ipv6 multicast limit cost	Applies a cost to mroutes that match per-interface mroute state limiters in IPv6.
ipv6 multicast limit rate	Configures the maximum allowed state on the source router.

ipv6 multicast limit cost

To apply a cost to mroutes that match per-interface mroute state limiters in IPv6, use t**he ipv6 multicast limit cost** command in global configuration mode. To restore the default cost for mroutes being limited by per-interface mroute state limiters, use the **no** form of this command.

ipv6 multicast [**vrf** *vrf-name*] **limit cost** *access-list cost-multiplier*

no ipv6 multicast [**vrf** *vrf-name*] **limit cost** *access-list cost-multiplier*

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
access-list	Access Control List (ACL) name that defines the mroutes for which to apply a cost.
cost-multiplier	Cost value applied to mroutes that match the corresponding ACL. The range is from 0 to 2147483647.

Command Default

If the **ipv6 multicast limit cost** command is not configured or if an mroute that is being limited by a per-interface mroute state limiter does not match any of the ACLs applied to **ipv6 multicast limit cost** command configurations, a cost of 1 is applied to the mroutes being limited.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.
Cisco IOS XE Release 2.6	This command was introduced on Cisco ASR 1000 series routers.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

Use the **ipv6 multicast limit cost** command to apply a cost to mroutes that match per-interface mroute state limiters (configured with the **ipv6 multicast limit** command in interface configuration mode). This command is primarily used to provide bandwidth-based Call Admission Control (CAC) in network environments where multicast flows utilize different amounts of bandwidth. Accordingly, when this command is configured, the configuration is usually referred to as a bandwidth-based multicast CAC policy.

The **ipv6 multicast limit cost** command complements the per-interface **ipv6 multicast limit** command. Once the *limit-acl* argument is matched in the **ipv6 multicast limit** command, the *access-list* argument in the **ipv6 multicast limit cost** command is checked to see which cost to apply to limited groups. If no cost match is found, the default cost is 1.

Examples

The following example configures the global limit on the source router.

```
Router(config)# ipv6 multicast limit cost costlist1 2
```

Related Commands

Command	Description
ipv6 multicast limit	Configures per-interface mroute state limiters in IPv6.

ipv6 multicast limit rate

To configure the maximum allowed state globally on the source router, use the **ipv6 multicast limit rate** command in global configuration mode. To remove the rate value, use the **no** form of this command.

ipv6 multicast limit rate *rate-value*

no ipv6 multicast limit rate *rate-value*

Syntax Description

rate-value	The maximum allowed state on the source router. The range is from 0 through 100.

Command Default

The maximum state is 1.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.

Usage Guidelines

The **ipv6 multicast rate limit** command is set to a maximum state of 1 message per second. If the default is set to 0, the syslog notification rate limiter is disabled.

Examples

The following example configures the maximum state on the source router:

```
ipv6 multicast limit rate 2
```

Related Commands

Command	Description
ipv6 multicast limit	Configures per-interface mroute state limiters in IPv6.

ipv6 multicast multipath

To enable load splitting of IPv6 multicast traffic across multiple equal-cost paths, use the **ipv6 multicast multipath** command in global configuration mode. To disable this function, use the **no** form of this command.

ipv6 multicast [**vrf** *vrf-name*] **multipath**

no ipv6 multicast [**vrf** *vrf-name*] **multipath**

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Default

This command is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

The **ipv6 multicast multipath** command is enabled by default. In the default scenario, the reverse path forwarding (RPF) neighbor is selected randomly from the available equal-cost RPF neighbors, resulting in the load splitting of traffic from different sources among the available equal cost paths. All traffic from a single source is still received from a single neighbor.

When the **no ipv6 multicast multipath** command is configured, the RPF neighbor with the highest IPv6 address is chosen for all sources with the same prefix, even when there are other available equal-cost paths.

Because the **ipv6 multicast multipath** command changes the way an RPF neighbor is selected, it must be configured consistently on all routers in a redundant topology to avoid looping.

Examples

The following example enables load splitting of IPv6 traffic:

```
Router(config)# ipv6 multicast multipath
```

Related Commands

Command	Description
show ipv6 rpf	Checks RPF information for a given unicast host address and prefix.

ipv6 multicast pim-passive-enable

To enable the Protocol Independent Multicast (PIM) passive feature on an IPv6 router, use the **ipv6 multicast pim-passive-enable** command in global configuration mode. To disable this feature, use the **no** form of this command.

ipv6 multicast pim-passive-enable

no ipv6 multicast pim-passive-enable

Syntax Description

This command has no arguments or keywords.

Command Default

PIM passive mode is not enabled on the router.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.

Usage Guidelines

Use the **ipv6 multicast pim-passive-enable** command to configure IPv6 PIM passive mode on a router. Once PIM passive mode is configured globally, use the **ipv6 pim passive** command in interface configuration mode to configure PIM passive mode on a specific interface.

Examples

The following example configures IPv6 PIM passive mode on a router:

```
Router(config)# ipv6 multicast pim-passive-enable
```

Related Commands

Command	Description
ipv6 pim passive	Configures PIM passive mode on a specific interface.

ipv6 multicast-routing

To enable multicast routing using Protocol Independent Multicast (PIM) and Multicast Listener Discovery (MLD) on all IPv6-enabled interfaces of the router and to enable multicast forwarding, use the **ipv6 multicast-routing** command in global configuration mode. To stop multicast routing and forwarding, use the **no** form of this command.

ipv6 multicast-routing [**vrf** *vrf-name*]

no ipv6 multicast-routing

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Default

Multicast routing is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
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.
12.2(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(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

Enabling IPv6 multicast on all interfaces also includes enabling PIM and MLD protocol processing on the interfaces. Users may configure specific interfaces before multicast is enabled, so that they can then disable PIM and MLD protocol processing on interfaces, as needed.

Examples

The following example enables multicast routing and turns on PIM and MLD on all interfaces:

```
ipv6 multicast-routing
```

Related Commands

Command	Description
ipv6 pim rp-address	Configures the address of a PIM RP for a particular group range.
no ipv6 pim	Turns off IPv6 PIM on a specified interface.
no ipv6 mld router	Disables MLD router-side processing on a specified interface.

ipv6 multicast rpf

To enable IPv6 multicast reverse path forwarding (RPF) check to use Border Gateway Protocol (BGP) unicast routes in the Routing Information Base (RIB), use the **ipv6 multicast rpf** command in global configuration mode. To disable this function, use the **no** form of this command.

ipv6 multicast [**vrf** *vrf-name*] **rpf** {**backoff** *initial-delay max-delay* | **use-bgp**}

no ipv6 multicast [**vrf** *vrf-name*] **rpf** {**backoff** *initial-delay max-delay* | **use-bgp**}

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
backoff	Specifies the backoff delay after a unicast routing change.
initial-delay	Initial RPF backoff delay, in milliseconds (ms). The range is from 200 to 65535.
max-delay	Maximum RPF backoff delay, in ms. The range is from 200 to 65535.
use-bgp	Specifies to use BGP routes for multicast RPF lookups.

Command Default

The multicast RPF check does not use BGP unicast routes.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(2)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.
12.2(33)SXI3	This command was integrated into Cisco IOS Release 12.2(33)SXI3.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The **backoff** keyword and *initial-delay max-delay* arguments were added.
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.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

When the **ipv6 multicast rpf** command is configured, multicast RPF check uses BGP unicast routes in the RIB. This is not done by default.

Examples

The following example shows how to enable the multicast RPF check function:

```
Router# configure terminal
Router(config)# ipv6 multicast rpf use-bgp
```

Related Commands

Command	Description
ipv6 multicast limit	Configure per-interface multicast route (mroute) state limiters in IPv6.
ipv6 multicast multipath	Enables load splitting of IPv6 multicast traffic across multiple equal-cost paths.

ipv6 nat

To designate that traffic originating from or destined for the interface is subject to Network Address Translation—Protocol Translation (NAT-PT), use the **ipv6 nat** command in interface configuration mode. To prevent the interface from being able to translate, use the **no** form of this command.

ipv6 nat

no ipv6 nat

Syntax Description

This command has no keywords or arguments.

Command Default

Traffic leaving or arriving at this interface is not subject to NAT-PT.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

The **ipv6 nat** command is usually specified on at least one IPv4 interface and one IPv6 interface at the networking device where you intend to use NAT-PT.

Examples

The following example assigns the IPv4 address 192.168.30.1 to Fast Ethernet interface 1/0 and the IPv6 address 2001:0DB8:0:1::1 to Fast Ethernet interface 2/0. IPv6 routing is globally enabled and both interfaces are configured to run IPv6 and enable NAT-PT translations.

```
interface fastethernet 1/0
 ip address 192.168.30.1 255.255.255.0
 ipv6 nat
!
interface fastethernet 2/0
 ipv6 address 2001:0DB8:0:1::1/64
 ipv6 nat
```

Related Commands

Command	Description
ipv6 address link-local	Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface.
ipv6 address eui-64	Configures an IPv6 address for an interface and enables IPv6 processing on an interface using an EUI-64 interface ID in the low-order 64 bits of the address.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.
show ipv6 nat translations	Displays active NAT-PT translations.

ipv6 nat max-entries

To specify the maximum number of Network Address Translation—Protocol Translation (NAT-PT) translation entries stored by the router, use the **ipv6 nat max-entries** command in global configuration mode. To restore the default number of NAT-PT entries, use the **no** form of this command.

ipv6 nat max-entries *number*

no ipv6 nat max-entries

Syntax Description

number	(Optional) Specifies the maximum number (1–2147483647) of NAT-PT translation entries. Default is unlimited.

Command Default

Unlimited number of NAT-PT entries.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

Use the **ipv6 nat max-entries** command to set the maximum number of NAT-PT translation entries stored by the router when the router memory is limited, or the actual number of translations is important.

Examples

The following example sets the maximum number of NAT-PT translation entries to 1000:

```
ipv6 nat max-entries 1000
```

Related Commands

Command	Description
clear ipv6 nat translation	Clears dynamic NAT-PT translations from the translation table.
show ipv6 nat translations	Displays active NAT-PT translations.

ipv6 nat prefix

To assign an IPv6 prefix where matching IPv6 packets will be translated using Network Address Translation—Protocol Translation (NAT-PT), use the **ipv6 nat prefix** command in global configuration or interface configuration mode. To prevent the IPv6 prefix from being used by NAT-PT, use the **no** form of this command.

ipv6 nat prefix *ipv6-prefix*/*prefix-length*

no ipv6 nat prefix *ipv6-prefix*/*prefix-length*

Syntax Description

ipv6-prefix	The IPv6 network used as the NAT-PT prefix. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/prefix-length	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). The only prefix length supported is 96. A slash mark must precede the decimal value.

Command Default

No IPv6 prefixes are used by NAT-PT.

Command Modes

Global configuration
Interface configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

The **ipv6 nat prefix** command is used to specify an IPv6 address prefix against which the destination prefix in an IPv6 packet is matched. If the match is successful, NAT-PT will translate the IPv6 packet to an IPv4 packet using the configured mapping rules.

Use the **ipv6 nat prefix** command in global configuration mode to assign a global NAT-PTNAT-PT prefix, or in interface configuration mode to assign a different NAT-PT prefix for each interface. Using a different NAT-PT prefix on several interfaces allows the NAT-PT router to support an IPv6 network with multiple exit points to IPv4 networks.

Examples

The following example assigns the IPv6 prefix 2001:0DB8:1::/96 as the global NAT-PT prefix:

```
ipv6 nat prefix 2001:0DB8:1::/96
```

The following example assigns the IPv6 prefix 2001:0DB8:2::/96 as the NAT-PT prefix for the Fast Ethernet interface 1/0, and the IPv6 prefix 2001:0DB8:4::/96 as the NAT-PT prefix for the Fast Ethernet interface 2/0:

```
interface fastethernet 1/0
 ipv6 address 2001:0DB8:2:1::1/64
 ipv6 nat prefix 2001:0DB8:2::/96
!
interface fastethernet 2/0
 ipv6 address 2001:0DB8:4:1::1/64
 ipv6 nat prefix 2001:0DB8:4::/96
```

Related Commands

Command	Description
ipv6 address link-local	Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface.
ipv6 address eui-64	Configures an IPv6 address for an interface and enables IPv6 processing on an interface using an EUI-64 interface ID in the low-order 64 bits of the address.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.
show ipv6 nat translations	Displays active NAT-PT translations.

ipv6 nat prefix v4-mapped

To enable customers to send traffic from their IPv6 network to an IPv4 network without configuring IPv6 destination address mapping, use the **ipv6 nat prefix v4-mapped** command in global configuration or interface configuration mode. To disable this feature, use the **no** form of this command.

ipv6 nat prefix *ipv6-prefix* **v4-mapped** {*access-list-name* | *ipv6-prefix*}

no ipv6 nat prefix *ipv6-prefix* **v4-mapped** {*access-list-name* | *ipv6-prefix*}

Syntax Description

ipv6-prefix	IPv6 prefix for Network Address Translation—Protocol Translation (NAT-PT).
access-list-name	Name of an IPv6 access list. Names cannot contain a space or quotation mark, or begin with a numeric.

Command Default

This command is not enabled.

Command Modes

Global configuration
Interface configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

The IPv6 target address of a packet arriving at an interface is checked to discover if it has a NAT-PT prefix that was configured with the **ipv6 nat prefix v4-mapped** command. If the prefix does match, then an access-list check is performed to discover if the source address matches the access list or prefix list. If the prefix does not match, the packet is dropped.

If the prefix matches, source address translation is performed. If a rule has been configured for the source address translation, the last 32 bits of the destination IPv6 address is used as the IPv4 destination and a flow entry is created.

Examples

In the following example, the access list permits any IPv6 source address with the prefix 2001::/96 to go to the destination with a 2000::/96 prefix. The destination is then translated to the last 32 bit of its IPv6 address; for example: source address = 2001::1, destination address = 2000::192.168.1.1. The destination then becomes 192.168.1.1 in the IPv4 network:

```
ipv6 nat prefix 2000::/96 v4-mapped v4map_acl

ipv6 access-list v4map_acl
 permit ipv6 2001::/96 2000::/96
```

ipv6 nat translation

To change the amount of time after which Network Address Translation—Protocol Translation (NAT-PT) translations time out, use the **ipv6 nat translation** command in global configuration mode. To disable the timeout, use the **no** form of this command.

ipv6 nat translation {**timeout** | **udp-timeout** | **dns-timeout** | **tcp-timeout** | **finrst-timeout** | **icmp-timeout** | **syn-timeout**} {*seconds* | **never**}

no ipv6 nat translation {**timeout** | **udp-timeout** | **dns-timeout** | **tcp-timeout** | **finrst-timeout** | **icmp-timeout** | **syn-timeout**}

Syntax Description

timeout	Specifies that the timeout value applies to dynamic translations. Default is 86400 seconds (24 hours).
udp-timeout	Specifies that the timeout value applies to the User Datagram Protocol (UDP) port. Default is 300 seconds (5 minutes).
dns-timeout	Specifies that the timeout value applies to connections to the Domain Naming System (DNS). Default is 60 seconds.
tcp-timeout	Specifies that the timeout value applies to the TCP port. Default is 86400 seconds (24 hours).
finrst-timeout	Specifies that the timeout value applies to Finish and Reset TCP packets, which terminate a connection. Default is 60 seconds.
icmp-timeout	Specifies the timeout value for Internet Control Message Protocol (ICMP) flows. Default is 60 seconds.
syn-timeout	Specifies that the timeout value applies when a TCP SYN (request to synchronize sequence numbers used when opening a connection) flag is received but the flag is not followed by data belonging to the same TCP session.
seconds	Number of seconds after which the specified translation timer expires. The default is 0.
never	Specifies that the dynamic translation timer never expires.

Command Default

timeout: 86400 seconds (24 hours)
udp-timeout: 300 seconds (5 minutes)
dns-timeout: 60 seconds (1 minute)
tcp-timeout: 86400 seconds (24 hours)
finrst-timeout: 60 seconds (1 minute)
icmp-timeout: 60 seconds (1 minute)

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

Dynamic translations time out after a period of time without any translations. The default timeout period is 24 hours. When port translation is configured, there is finer control over translation entry timeouts because each entry contains more context about the traffic that is using it. Non-DNS UDP translations time out after 5 minutes, and DNS times out in 1 minute. TCP translations time out in 24 hours, unless an RST or FIN flag is seen on the stream, in which case they will time out in 1 minute.

Examples

The following example causes UDP port translation entries to time out after 10 minutes:

```
ipv6 nat translation udp-timeout 600
```

Related Commands

Command	Description
clear ipv6 nat translation	Clears dynamic NAT-PT translations from the translation table.
show ipv6 nat translations	Displays active NAT-PT translations.

ipv6 nat v4v6 pool

To define a pool of IPv6 addresses for Network Address Translation—Protocol Translation (NAT-PT), use the **ipv6 nat v4v6 pool** command in global configuration mode. To remove one or more addresses from the pool, use the **no** form of this command.

ipv6 nat v4v6 pool *name start-ipv6 end-ipv6* **prefix-length** *prefix-length*

no ipv6 nat v4v6 pool *name start-ipv6 end-ipv6* **prefix-length** *prefix-length*

Syntax Description

name	Name of the pool.
start-ipv6	Starting IPv6 address that defines the range of IPv6 addresses in the address pool.
end-ipv6	Ending IPv6 address that defines the range of IPv6 addresses in the address pool.
prefix-length *prefix-length*	Number that indicates how many bits of the address indicate the network. Specify the subnet of the network to which the pool addresses belong.

Command Default

No pool of addresses is defined.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

This command defines a pool of IPv6 addresses using start address, end address, and prefix length. The pool is used when NAT-PT needs a dynamic mapping of an IPv6 address to translate an IPv4 address.

Examples

The following example configures a dynamic NAT-PT mapping to translate IPv4 addresses to IPv6 addresses using a pool of IPv6 addresses named v6pool. The packets to be translated by NAT-PT are filtered using an access list named pt-list2. One static NAT-PT mapping is configured to access a Domain Naming System (DNS) server. Ethernet interface 3/1 is an IPv6-only host and Ethernet interface 3/3 is an IPv4-only host.

```
interface Ethernet3/1
 ipv6 address 2001:0DB8:AABB:1::9/64
 ipv6 enable
 ipv6 nat
!
interface Ethernet3/3
 ip address 192.168.30.9 255.255.255.0
 ipv6 nat
!
ipv6 nat v4v6 source list pt-list2 pool v6pool
ipv6 nat v4v6 pool v6pool 2001:0DB8:EEFF::1 2001:0DB8:EEFF::2 prefix-length 128
ipv6 nat v6v4 source 2001:0DB8:AABB:1::1 10.21.8.0
```

```
ipv6 nat prefix 2001:0DB8:EEFF::/96
!
access-list pt-list2 permit 192.168.30.0 0.0.0.255
```

Related Commands

Command	Description
clear ipv6 nat translations	Clears dynamic NAT-PT translations from the translation table.
show ipv6 nat translations	Displays active NAT-PT translations.

ipv6 nat v4v6 source

To configure IPv4 to IPv6 address translation using Network Address Translation—Protocol Translation (NAT-PT), use the **ipv6 nat v4v6 source** command in global configuration mode. To remove the static translation or remove the dynamic association to a pool, use the **no** form of this command.

ipv6 nat v4v6 source {**list** {*access-list-number* | *name*} **pool** *name* | *ipv4-address ipv6-address*}

no ipv6 nat v4v6 source {**list** {*access-list-number* | *name*} **pool** *name* | *ipv4-address ipv6-address*}

Syntax Description

list *access-list-number*	Standard IP access list number. Packets with source addresses that pass the access list are dynamically translated using global addresses from the named pool.
list *name*	Name of a standard IP access list. Packets with source addresses that pass the access list are dynamically translated using global addresses from the named pool.
pool *name*	Name of the pool from which global IP addresses are allocated dynamically.
ipv4-address	Sets up a single static translation. This argument establishes the local IP address assigned to a host on the inside network. The address could be randomly chosen, allocated from RFC 1918, or obsolete.
ipv6-address	Sets up a single static translation. This argument establishes the globally unique IP address of an inside host as it appears to the outside world.

Command Default

No NAT-PT translation of IPv4 to IPv6 addresses occurs.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

This command has two forms: dynamic and static address translation. The form with an IPv6 access list establishes dynamic translation. Packets from IPv4 addresses that match the standard access list are translated using IPv6 addresses allocated from the pool named with the **ipv6 nat v4v6 pool** command. The access list is used to specify which traffic is to be translated.

Alternatively, the syntax form using the *ipv4-address* and *ipv6-address* arguments establishes a single static translation.

Examples

The following example configures a dynamic NAT-PT mapping to translate IPv4 addresses to IPv6 addresses using a pool of IPv6 addresses named v6pool. The packets to be translated by NAT-PT are filtered using an access list named pt-list2. Ethernet interface 3/1 is an IPv6-only host and Ethernet interface 3/3 is an IPv4-only host.

```
interface Ethernet3/1
 ipv6 address 2001:0DB8:AABB:1::9/64
 ipv6 enable
 ipv6 nat
!
interface Ethernet3/3
 ip address 192.168.30.9 255.255.255.0
 ipv6 nat
!
ipv6 nat v4v6 source list pt-list2 pool v6pool
ipv6 nat v4v6 pool v6pool 2001:0DB8:EEFF::1 2001:0DB8:EEFF::2 prefix-length 128
ipv6 nat prefix 3ffe:c00:yyyy::/96
!
access-list pt-list2 permit 192.168.30.0 0.0.0.255
```

The following example shows a static translation where the IPv4 address 192.168.30.1 is translated into the IPv6 address 2001:0DB8:EEFF::2:

```
ipv6 nat v4v6 source 192.168.30.1 2001:0DB8:EEFF::2
```

Related Commands

Command	Description
clear ipv6 nat translation	Clears dynamic NAT-PT translations from the translation state table.
ipv6 nat v4v6 pool	Defines a pool of IPv6 addresses for NAT-PT.
ipv6 nat v6v4 source	Enables NAT-PT for an IPv6 source address.
show ipv6 nat translations	Displays active NAT-PT translations.

ipv6 nat v6v4 pool

To define a pool of IPv4 addresses for Network Address Translation—Protocol Translation (NAT-PT), use the **ipv6 nat v6v4 pool** global configuration command. To remove one or more addresses from the pool, use the **no** form of this command.

ipv6 nat v6v4 pool *name start-ipv4 end-ipv4* **prefix-length** *prefix-length*

no ipv6 nat v6v4 pool *name start-ipv4 end-ipv4* **prefix-length** *prefix-length*

Syntax Description

name	Name of the pool.
start-ipv4	Starting IPv4 address that defines the range of IPv4 addresses in the address pool.
end-ipv4	Ending IPv4 address that defines the range of IPv4 addresses in the address pool.
prefix-length *prefix-length*	Number that indicates how many bits of the address indicate the network. Specify the subnet of the network to which the pool addresses belong.

Command Default

No pool of addresses is defined.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

This command defines a pool of IPv4 addresses using start address, end address, and prefix length. The pool is used when NAT-PT needs a dynamic mapping of IPv4 addresses to translate IPv6 addresses.

Examples

The following example configures a dynamic NAT-PT mapping to translate IPv6 addresses to IPv4 addresses using a pool of IPv4 addresses named v4pool. The packets to be translated by NAT-PT are filtered using an IPv6 access list named pt-list1. One static NAT-PT mapping is configured to access a Domain Naming System (DNS) server. Ethernet interface 3/1 is an IPv6-only host and Ethernet interface 3/3 is an IPv4-only host.

```
interface Ethernet3/1
 ipv6 address 2001:0DB8:AABB:1::9/64
 ipv6 enable
 ipv6 nat
!
interface Ethernet3/3
 ip address 192.168.30.9 255.255.255.0
 ipv6 nat
!
ipv6 nat v4v6 source 192.168.30.1 2001:0DB8:EEFF::2
ipv6 nat v6v4 source list pt-list1 pool v4pool
ipv6 nat v6v4 pool v4pool 10.21.8.1 10.21.8.10 prefix-length 24
```

```
ipv6 nat prefix 2001:0DB8:EEFF::/96
!
ipv6 access-list pt-list1
 permit ipv6 2001:0DB8:AABB:1::/64 any
```

Related Commands

Command	Description
clear ipv6 nat translations	Clears dynamic NAT-PT translations from the translation table.
show ipv6 nat translations	Displays active NAT-PT translations.

ipv6 nat v6v4 source

To configure IPv6 to IPv4 address translation using Network Address Translation—Protocol Translation (NAT-PT), use the **ipv6 nat v6v4 source** command in global configuration mode. To remove the static translation or remove the dynamic association to a pool, use the **no** form of this command.

ipv6 nat v6v4 source {**list** *access-list-name* **pool** *name* | **route-map** *map-name* **pool** *name* | *ipv6-address ipv4-address*} [**overload**]

no ipv6 nat v6v4 source {**list** *access-list-name* **pool** *name* | **route-map** *map-name* **pool** *name* | *ipv6-address ipv4-address*} [**overload**]

Syntax Description

list *access-list-name*	IPv6 access list name. Packets with source addresses that pass the access list are translated using global addresses from the named pool.
route-map *map-name*	Sets up a single static translation. This keyword and argument combination establishes the globally unique IP address assigned to a host on the outside network by its owner. It was allocated from globally routable network space.
pool *name*	Name of the pool from which global IP addresses are allocated dynamically.
ipv6-address	Sets up a single static translation. This argument establishes the globally unique IP address of an inside host as it appears to the outside world.
ipv4-address	Sets up a single static translation. This argument establishes the local IP address assigned to a host on the inside network. The address could be randomly chosen, allocated from RFC 1918, or obsolete.
overload	Enables multiplexing of IPv6 addresses to a single IPv4 address for TCP, UDP, and ICMD.

Command Default

No NAT-PT translation of IPv6 to IPv4 addresses occurs.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.3(2)T	The **overload** keyword was added to support Port Address Translation (PAT), or Overload, multiplexing multiple IPv6 addresses to a single IPv4 address or to an IPv4 address pool.

Usage Guidelines

Dynamic and Static Address Translation

This command has two forms: dynamic and static address translation. The form with an IPv6 access list establishes dynamic translation. Packets from IPv6 addresses that match the IPv6 access list are translated using IPv4 addresses allocated from the pool named with the **ipv6 nat v6v4 pool** command. The access list is used to specify which traffic is to be translated.

Alternatively, the syntax form using the *ipv6-address* and *ipv4-address* arguments establishes a single static translation.

Port Address Translation

When used for PAT, the command can be used for a single IPv4 interface or for a pool of IPv4 interfaces.

Examples

Dynamic Mapping to a Pool of IPv4 Addresses Example

The following example configures a dynamic NAT-PT mapping to translate IPv6 addresses to IPv4 addresses using a pool of IPv4 addresses named v4pool. The packets to be translated by NAT-PT are filtered using an IPv6 access list named pt-list1. Ethernet interface 3/1 is an IPv6-only host and Ethernet interface 3/3 is an IPv4-only host.

```
interface Ethernet3/1
 ipv6 address ffe:aaaa:bbbb:1::9/64
 ipv6 enable
 ipv6 nat
!
interface Ethernet3/3
 ip address 192.168.30.9 255.255.255.0
 ipv6 nat
!
ipv6 nat v6v4 source list pt-list1 pool v4pool
ipv6 nat v6v4 pool v4pool 10.21.8.1 10.21.8.10 prefix-length 24
ipv6 nat prefix 3ffe:c00:::/96
!
ipv6 access-list pt-list1
 permit ipv6 3ffe:aaaa:bbbb:1::/64 any
```

Static Translation for a Single Address Example

The following example shows a static translation where the IPv6 address 3ffe:aaaa:bbbb:1::1 is translated into the IPv4 address 10.21.8.10:

```
ipv6 nat v6v4 source 3ffe:aaaa:bbbb:1::1 10.21.8.10
```

Port Address Translation to a Single Address Example

```
ipv6 nat v6v4 pool v6pool 10.1.1.1 10.1.1.10 subnetmask 255.255.255.0
ipv6 nat v6v4 source list v6list interface e1 overload
ipv6 accesslist v6list
permit 3000::/64 any
```

Related Commands

Command	Description
clear ipv6 nat translation	Clears dynamic NAT-PT translations from the translation state table.
debug ipv6 nat	Displays debugging messages for NAT-PT.
ipv6 nat v6v4 pool	Defines a pool of IPv4 addresses for NAT-PT.
ipv6 nat v4v6 source	Enables NAT-PT for an IPv4 source address.
show ipv6 nat translations	Displays active NAT-PT translations.

ipv6 nd advertisement-interval

To configure the advertisement interval option in router advertisements (RAs), use the **ipv6 nd advertisement-interval** in interface configuration mode. To reset the interval to the default value, use the **no** form of this command.

ipv6 nd advertisement-interval

no ipv6 nd advertisement-interval

Syntax Description

This command has no arguments or keywords.

Command Default

Advertisement interval option is not sent.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

Use the **ipv6 nd advertisement-interval** command to indicate to a visiting mobile node the interval at which that node may expect to receive RAs. The node may use this information in its movement detection algorithm.

Examples

The following example enables the advertisement interval option to be sent in RAs:

```
Router(config-if)# ipv6 nd advertisement-interval
```

Related Commands

Command	Description
ipv6 mobile home-agent (interface configuration)	Initializes and starts the Mobile IPv6 home agent on a specific interface.
ipv6 nd ra-interval	Configures the interval between Mobile IPv6 RA transmissions on an interface.

ipv6 nd cache expire

To configure the length of time before an IPv6 ND cache entry expires, use the **ipv6 nd cache expire** command in interface configuration mode. To remove this configuration, use the **no** form of this command.

ipv6 nd cache expire *expire-time-in-seconds* [**refresh**]

no ipv6 nd cache expire *expire-time-in-seconds* [**refresh**]

Syntax Description

expire-time-in-seconds	The range is from 1 through 65536 seconds. The default is 14,400 seconds, or 4 hours.
refresh	(Optional) Automatically refreshes the ND cache entry.

Command Default

14,400 seconds (4 hours)

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI7	This command was introduced.

Usage Guidelines

By default, an ND cache entry is expired and deleted if it remains in the STALE state for 14,400 seconds, or 4 hours. The **ipv6 nd cache expire** command allows the user to vary the expiry time and to trigger auto-refresh of an expired entry before the entry is deleted.

When the **refresh** keyword is used, an ND cache entry is autorefreshed. The entry moves into the DELAY state and the neighbor unreachability detection (NUD) process occurs, in which the entry transitions from the DELAY state to the PROBE state after 5 seconds. When the entry reaches the PROBE state, a neighbor solicitation (NS) is sent and then retransmitted as per the configuration.

Examples

The following example shows the ND cache entry is configured to expire in 7200 seconds, or 2 hours:

```
Router(config-if)# ipv6 nd cache expire 7200
```

ipv6 nd cache interface-limit (global)

To configure a neighbor discovery cache limit on all interfaces on the router, use the **ipv6 nd cache interface-limit** command in global configuration mode. To remove the neighbor discovery from all interfaces on the router, use the **no** form of this command.

ipv6 nd cache interface-limit *size* [**log** *rate*]

no ipv6 nd cache interface-limit *size* [**log** *rate*]

Syntax Description

size	Cache size.
log *rate*	(Optional) Adjustable logging rate, in seconds. The valid values are 0 and 1.

Command Default

Default logging rate for the router is one entry every second.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T.

Usage Guidelines

The **ipv6 nd cache interface-limit** command in global configuration mode imposes a common per-interface cache size limit on all interfaces on the router.

Issuing the **no** or default form of the command will remove the neighbor discovery limit from every interface on the router that was configured using global configuration mode. It will not remove the neighbor discovery limit from any interface configured using the **ipv6 nd cache interface-limit** command in interface configuration mode.

The default (and maximum) logging rate for the router is one entry every second.

Examples

The following example shows how to set a common per-interface cache size limit of 4 seconds on all interfaces on the router:

```
Router(config)# ipv6 nd cache interface-limit 4
```

Related Commands

Command	Description
ipv6 nd cache interface-limit (interface)	Configures a neighbor discovery cache limit on a specified interface on the router.

ipv6 nd cache interface-limit (interface)

To configure a neighbor discovery cache limit on a specified interface on the router, use the **ipv6 nd cache interface-limit** command in interface configuration mode. To remove the neighbor discovery limit configured through interface configuration mode from the interface, use the **no** form of this command.

ipv6 nd cache interface-limit *size* [**log** *rate*]

no ipv6 nd cache interface-limit *size* [**log** *rate*]

Syntax Description

size	Cache size.
log *rate*	(Optional) Adjustable logging rate, in seconds. The valid values are 0 and 1.

Command Default

Default logging rate for the router is one entry every second.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T.

Usage Guidelines

The **ipv6 nd cache interface-limit** command in interface configuration mode allows you to configure a per-interface neighbor discovery limit on the associated interface. The limit configured by this command overrides any limit configured using the **ipv6 nd cache interface-limit** command in global configuration mode.

Issuing the **no** or default form of the command removes the neighbor discovery limit configured using interface configuration mode from the interface. Then, if the **ipv6 nd cache interface-limit** command in global configuration mode has been issued, the neighbor discovery limit on the interface reverts to that specified by global configuration. If the globally configured limit is smaller than the interface limit, then excess entries are removed. If the **ipv6 nd cache interface-limit** command in global configuration mode has not been issued, then no limit is set on the interface.

The number of entries in the neighbor discovery cache is limited on an interface basis. Once the limit is reached, no new entries are allowed.

Examples

The following example shows how to set the number of entries in a neighbor discovery cache (on an interface basis) to 1:

```
Router(config-if)# ipv6 nd cache interface-limit 1
```

Related Commands

Command	Description
ipv6 nd cache interface-limit (global)	Configures a neighbor discovery cache limit on all interfaces on the routers.

ipv6 nd dad attempts

To configure the number of consecutive neighbor solicitation messages that are sent on an interface while duplicate address detection is performed on the unicast IPv6 addresses of the interface, use the **ipv6 nd dad attempts** command in interface configuration mode. To return the number of messages to the default value, use the **no** form of this command.

ipv6 nd dad attempts *value*

no ipv6 nd dad attempts *value*

Syntax Description

value	The number of neighbor solicitation messages. The acceptable range is from 0 to 600. Configuring a value of 0 disables duplicate address detection processing on the specified interface; a value of 1 configures a single transmission without follow-up transmissions. Default is one message.

Command Default

Duplicate address detection on unicast IPv6 addresses with the sending of one neighbor solicitation message is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(4)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 Release 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.

Usage Guidelines

Duplicate address detection verifies the uniqueness of new unicast IPv6 addresses before the addresses are assigned to interfaces (the new addresses remain in a tentative state while duplicate address detection is performed). Duplicate address detection uses neighbor solicitation messages to verify the uniqueness of unicast IPv6 addresses.

The DupAddrDetectTransmits node configuration variable (as specified in RFC 2462, *IPv6 Stateless Address Autoconfiguration*) is used to automatically determine the number of consecutive neighbor solicitation messages that are sent on an interface while duplicate address detection is performed on a tentative unicast IPv6 address.

The interval between duplicate address detection, neighbor solicitation messages (the duplicate address detection timeout interval) is specified by the neighbor discovery-related variable RetransTimer (as specified in RFC 2461, *Neighbor Discovery for IP Version 6 [IPv6]*), which is used to determine the time between retransmissions of neighbor solicitation messages to a neighbor when resolving the address or

when probing the reachability of a neighbor. This is the same management variable used to specify the interval for neighbor solicitation messages during address resolution and neighbor unreachability detection. Use the **ipv6 nd ns-interval** command to configure the interval between neighbor solicitation messages that are sent during duplicate address detection.

Duplicate address detection is suspended on interfaces that are administratively "down." While an interface is administratively "down," the unicast IPv6 addresses assigned to the interface are set to a pending state. Duplicate address detection is automatically restarted on an interface when the interface returns to being administratively "up."

Note An interface returning to administratively "up" restarts duplicate address detection for all of the unicast IPv6 addresses on the interface. While duplicate address detection is performed on the link-local address of an interface, the state for the other IPv6 addresses is still set to TENTATIVE. When duplicate address detection is completed on the link-local address, duplicate address detection is performed on the remaining IPv6 addresses.

When duplicate address detection identifies a duplicate address, the state of the address is set to DUPLICATE and the address is not used. If the duplicate address is the link-local address of the interface, the processing of IPv6 packets is disabled on the interface and an error message similar to the following is issued:

```
%IPV6-4-DUPLICATE: Duplicate address FE80::1 on Ethernet0
```

If the duplicate address is a global address of the interface, the address is not used and an error message similar to the following is issued:

```
%IPV6-4-DUPLICATE: Duplicate address 3000::4 on Ethernet0
```

All configuration commands associated with the duplicate address remain as configured while the state of the address is set to DUPLICATE.

If the link-local address for an interface changes, duplicate address detection is performed on the new link-local address and all of the other IPv6 address associated with the interface are regenerated (duplicate address detection is performed only on the new link-local address).

Duplicate address detection is performed on all multicast-enabled IPv6 interfaces, including the following interface types:

- ATM permanent virtual circuit (PVC)
- Cisco High-Level Data Link Control (HDLC)
- Ethernet, Fast Ethernet, and Gigabit Ethernet
- FDDI
- Frame Relay PVC
- Point-to-point links
- PPP

Examples

The following example configures five consecutive neighbor solicitation messages to be sent on Ethernet interface 0 while duplicate address detection is being performed on the tentative unicast IPv6 address of the interface. The example also disables duplicate address detection processing on Ethernet interface 1.

```
Router(config)# interface ethernet 0
Router(config-if)# ipv6 nd dad attempts 5
```

```
Router(config)# interface ethernet 1
Router(config-if)# ipv6 nd dad attempts 0
```

Note Configuring a value of 0 with the **ipv6 nd dad attempts** command disables duplicate address detection processing on the specified interface; a value of 1 configures a single transmission without follow-up transmissions. The default is one message.

To display the state (OK, TENTATIVE, or DUPLICATE) of the unicast IPv6 address configured for an interface, to verify whether duplicate address detection is enabled on the interface, and to verify the number of consecutive duplicate address detection, neighbor solicitation messages that are being sent on the interface, enter the **show ipv6 interface** command:

```
Router# show ipv6 interface

Ethernet0 is up, line protocol is up
  IPv6 is stalled, link-local address is FE80::1 [TENTATIVE]
  Global unicast address(es):
    2000::1, subnet is 2000::/64 [TENTATIVE]
    3000::1, subnet is 3000::/64 [TENTATIVE]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses.

Ethernet1 is up, line protocol is up
  IPv6 is stalled, link-local address is FE80::2
  Global unicast address(es):
    2000::2, subnet is 2000::/64
    3000::3, subnet is 3000::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is disabled, number of DAD attempts: 0
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses.
```

Related Commands

Command	Description
ipv6 nd ns-interval	Configures the interval between IPv6 neighbor solicitation transmissions on an interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd dad time

To configure the neighbor solicitation (NS) retransmit interval for duplicate address detection (DAD) separately from the NS retransmit interval for address resolution, use the **ipv6 nd dad time** command in global configuration or interface configuration mode. To remove the NS retransmit interval for DAD, use the **no** form of this command.

ipv6 nd dad time *milliseconds*

no ipv6 nd dad time

Syntax Description

milliseconds	The interval between IPv6 neighbor solicit transmissions for DAD. The range is from 1000 to 3600000 milliseconds.

Command Default

Default NS retransmit interval: 1000 msec (1 second)

Command Modes

Global configuration (config)
Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 3S	This command was introduced.

Usage Guidelines

The **ipv6 nd dad time** command allows you to configure the NS retransmit interval for DAD separately from the NS retransmit interval for address resolution. This command also allows you to set the behavior globally for the whole router or on a per-interface basis.

Examples

The following example shows how to increase the default NS retransmit interval on an interface for address resolution to 3 seconds but keep the DAD NS retransmit interval at the default value of 1 second:

```
Router(config-if)# ipv6 nd ns-interval 3000
Router(config-if)# ipv6 nd dad time 1000
```

Related Commands

Command	Description
ipv6 nd ns-interval	Configures the interval between IPv6 neighbor solicitation retransmissions for address resolution on an interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd inspection

To apply the Neighbor Discovery Protocol (NDP) inspection feature, use the **ipv6 nd inspection** command in interface configuration mode. To remove the NDP inspection feature, use the **no** form of this command.

ipv6 nd inspection [**attach-policy** [**policy** *policy-name*] | **vlan** {**add** | **except** | **none** | **remove** | **all**} *vlan* [*vlan1, vlan2, vlan3*...]]]

no ipv6 nd inspection

Syntax Description

attach-policy	(Optional) Attaches an NDP Inspection policy.
policy-name	(Optional) The NDP Inspection policy name.
vlan	(Optional) Applies the ND inspection feature to a VLAN on the interface.
add	Adds a VLAN to be inspected.
except	All VLANs are inspected except the one specified.
none	No VLANs are inspected.
remove	Removes the specified VLAN from NDP inspection.
all	NDP traffic from all VLANs on the port is inspected.
vlan	(Optional) A specific VLAN on the interface. More than one VLAN can be specified (*vlan1*, *vlan2*, *vlan3*...). The VLAN number that can be used is from 1 through 4094.

Command Default

All NDP messages are inspected.
Secure Neighbor Discovery (SeND) options are ignored.
Neighbors are probed based on the criteria defined in neighbor tracking feature.
Per-port IPv6 address limit enforcement is disabled.
Layer 2 header source MAC address validations are disabled.
Per-port rate limiting of the NDP messages in software is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

The **ipv6 nd inspection** command applies the NDP Inspection feature on a specified interface. If the user enables the optional **attach-policy** or **vlan** keywords, NDP traffic is inspected by policy or by VLAN. If no VLANs are specified, NDP traffic from all VLANs on the port is inspected (which is equivalent to using the **vlan all** keywords).

If no policy is specified in this command, the default criteria are as follows:

- All NDP messages are inspected.

- SeND options are ignored.
- Neighbors are probed based on the criteria defined in neighbor tracking feature.
- Per-port IPv6 address limit enforcement is disabled.
- Layer 2 header source MAC address validations are disabled.
- Per-port rate limiting of the NDP messages in software is disabled.

If a VLAN is specified, its parameter is either a single VLAN number from 1 through 4094 or a range of VLANs described by two VLAN numbers, the lesser one first, separated by a dash (for example, **vlan 1-100,200,300-400**). Do not enter any spaces between comma-separated VLAN parameters or in dash-specified ranges.

Examples

The following example enables NDP inspection on a specified interface:

```
Router(config-if)# ipv6 nd inspection
```

ipv6 nd inspection policy

To define the Neighbor Discovery ND inspection policy name and enter ND inspection policy configuration mode, use the **ipv6 nd inspection** command in global configuration mode. To remove the ND inspection policy, use the **no** form of this command.

ipv6 nd inspection policy *policy-name*

no ipv6 nd inspection policy *policy-name*

Syntax Description

policy-name	The ND inspection policy name.

Command Default

No ND inspection policies are configured.

Command Modes

ND inspection configuration (config-nd-inspection)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

The **ipv6 nd inspection policy** command defines the ND inspection policy name, and enters the router into ND inspection policy configuration mode. Once you are in ND inspection policy configuration mode, you can use any of the following subcommands:

- **device-role**
- **drop-unsecure**
- **limit address-count**
- **sec-level minimum**
- **tracking**
- **trusted-port**
- **validate source-mac**

Examples

The following example defines an ND policy name as policy1:

```
Router(config)# ipv6 nd inspection policy policy1
Router(config-nd-inspection)#
```

Related Commands

Command	Description
device-role	Specifies the role of the device attached to the port.
drop-unsecure	Drops messages with no or invalid options or an invalid signature.

Command	Description
limit address-count	Limits the number of IPv6 addresses allowed to be used on the port.
sec-level minimum	Specifies the minimum security level parameter value when CGA options are used.
tracking	Overrides the default tracking policy on a port.
trusted-port	Configures a port to become a trusted port.
validate source-mac	Checks the source MAC address against the link-layer address.

ipv6 nd managed-config-flag

To set the "managed address configuration flag" in IPv6 router advertisements, use the **ipv6 nd managed-config-flag** command in interface configuration mode. To clear the flag from IPv6 router advertisements, use the **no** form of this command.

ipv6 nd managed-config-flag

no ipv6 nd managed-config-flag

Syntax Description

This command has no arguments or keywords.

Command Default

The "managed address configuration flag" flag is not set in IPv6 router advertisements.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)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 Release 12.2(14)S.
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.
12.2(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

Setting the "managed address configuration flag" flag in IPv6 router advertisements indicates to attached hosts whether they should use stateful autoconfiguration to obtain addresses. If the flag is set, the attached hosts should use stateful autoconfiguration to obtain addresses. If the flag is not set, the attached hosts should not use stateful autoconfiguration to obtain addresses.

Hosts may use stateful and stateless address autoconfiguration simultaneously.

Examples

The following example configures the "managed address configuration flag" flag in IPv6 router advertisements on Ethernet interface 0/0:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 nd managed-config-flag
```

Related Commands

Command	Description
ipv6 nd prefix-advertisement	Configures which IPv6 prefixes are included in IPv6 router advertisements
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd na glean

To configure Neighbor Discovery (ND) to glean an entry from an unsolicited neighbor advertisement (NA), use the **ipv6 nd na glean** command in interface configuration mode. To disable this feature, use the **no** form of this command.

ipv6 nd na glean

no ipv6 nd na glean

Syntax Description

This command has no arguments or keywords.

Command Default

The router ignores an unsolicited NA.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI7	This command was introduced.

Usage Guidelines

IPv6 nodes may choose to emit a multicast unsolicited NA packet following the successful completion of duplicate address detection (DAD). By default, these unsolicited NA packets are ignored by other IPv6 nodes. The **ipv6 nd na glean** command configures the router to create an ND entry on receipt of an unsolicited NA packet (assuming no such entry already exists and the NA has the link-layer address option). Use of this command allows a router to prepopulate its ND cache with an entry for a neighbor in advance of any data traffic exchange with the neighbor.

Examples

The following example configures ND to glean an entry from an unsolicited neighbor advertisement:

```
Router(config-if)# ipv6 nd na glean
```

ipv6 nd ns-interval

To configure the interval between IPv6 neighbor solicitation (NS) retransmissions on an interface, use the **ipv6 nd ns-interval** command in interface configuration mode. To restore the default interval, use the **no** form of this command.

ipv6 nd ns-interval *milliseconds*

no ipv6 nd ns-interval

Syntax Description

milliseconds	The interval between IPv6 neighbor solicit transmissions for address resolution. The acceptable range is from 1000 to 3600000 milliseconds.

Command Default

0 milliseconds (unspecified) is advertised in router advertisements and the value 1000 is used for the neighbor discovery activity of the router itself.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(2)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 Release 12.2(14)S.
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.
12.2(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

By default, using the **ipv6 nd ns-interval** command changes the NS retransmission interval for both address resolution and duplicate address detection (DAD). To specify a different NS retransmission interval for DAD, use the **ipv6 nd dad time** command.

This value will be included in all IPv6 router advertisements sent out this interface. Very short intervals are not recommended in normal IPv6 operation. When a nondefault value is configured, the configured time is both advertised and used by the router itself.

Examples

The following example configures an IPv6 neighbor solicit transmission interval of 9000 milliseconds for Ethernet interface 0/0:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 nd ns-interval 9000
```

Related Commands

Command	Description
ipv6 nd dad time	Configures the NS retransmit interval for DAD separately from the NS retransmit interval for address resolution.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd nud retry

To configure the number of times neighbor unreachability detection (NUD) resends neighbor solicitations (NSs), use the **ipv6 nd nud retry** command in interface configuration mode. To disable this feature, use the **no** form of this command.

ipv6 nd nud retry *base interval max-attempts*

no ipv6 nd nud retry *base interval max-attempts*

Syntax Description

base	The base NUD value.
interval	The time interval, in milliseconds, between retries.
max-attempts	The maximum number of retry attempts, depending on the base value.

Command Default

Three NS packets are sent 1 second apart.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI7	This command was introduced.

Usage Guidelines

When a router runs NUD to re-resolve the ND entry for a neighbor, it sends three NS packets 1 second apart. In certain situations (e.g., spanning-tree events, high traffic, the end host being reloaded), three NS packets sent at an interval of 1 second may not be sufficient. To help maintain the neighbor cache in such situations, use the **ipv6 nd nud retry** command to configure exponential timers for NS retransmits.

The maximum number of retry attempts is configured using the *max-attempts* argument. The retransmit interval is calculated with the following formula:

tm^n

- t = Time interval
- m = Base (1, 2, or 3)
- n = Current NS number (where the first NS is 0)

The **ipv6 nd nud retry** command only affects the retransmit rate for NUD, not for initial resolution, which uses the default of 3 NS packets sent 1 second apart.

Examples

The following example provides a fixed interval of 1 second and three retransmits:

```
Router(config-if)# ipv6 nd nud retry 1 1000 3
```

The following example provides a retransmit interval of 1, 2, 4, and 8:

```
Router(config-if)# ipv6 nd nud retry 2 1000 4
```

The following example provides the retransmit intervals of 1, 3, 9, 27, 81:

```
Router(config-if)# ipv6 nd nud retry 3 1000 5
```

ipv6 nd other-config-flag

To set the "other stateful configuration" flag in IPv6 router advertisements, use the **ipv6 nd other-config-flag** command in interface configuration mode. To clear the flag from IPv6 router advertisements, use the **no** form of this command.

ipv6 nd other-config-flag

no ipv6 nd other-config-flag

Syntax Description

This command has no arguments or keywords.

Command Default

The "other stateful configuration" flag is not set in IPv6 router advertisements.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)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 Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
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.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

The setting of the "other stateful configuration" flag in IPv6 router advertisements indicates to attached hosts how they can obtain autoconfiguration information other than addresses. If the flag is set, the attached hosts should use stateful autoconfiguration to obtain the other (nonaddress) information.

Note If the "managed address configuration" flag is set using the **ipv6 nd managed-config-flag** command, then an attached host can use stateful autoconfiguration to obtain the other (nonaddress) information regardless of the setting of the "other stateful configuration" flag.

Examples

The following example configures the "other stateful configuration" flag in IPv6 router advertisements on Ethernet interface 0/0:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 nd other-config-flag
```

Related Commands

Command	Description
ipv6 nd managed-config-flag	Sets the "managed address configuration" flag in IPv6 router advertisements.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd prefix

To configure which IPv6 prefixes are included in IPv6 Neighbor Discovery (ND) router advertisements, use the **ipv6 nd prefix** command in interface configuration mode. To remove the prefixes, use the **no** form of this command.

ipv6 nd prefix {*ipv6-prefix*/*prefix-length* | **default**} [**no-advertise** | [*valid-lifetime preferred-lifetime* [**off-link** | **no-rtr-address** | **no-autoconfig** | **no-onlink**]]] | [**at** *valid-date* | *preferred-date* [**off-link** | **no-rtr-address** | **no-autoconfig**]]

no ipv6 nd prefix {*ipv6-prefix*/*prefix-length* | **default**}

Syntax Description

ipv6-prefix	The IPv6 network number to include in router advertisements. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/*prefix-length*	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
default	Default values are used.
no-advertise	(Optional) The prefix is not advertised.
valid-lifetime	(Optional) The amount of time (in seconds) that the specified IPv6 prefix is advertised as being valid.
preferred-lifetime	(Optional) The amount of time (in seconds) that the specified IPv6 prefix is advertised as being preferred.
off-link	(Optional) Configures the specified prefix as off-link. The prefix will be advertised with the L-bit clear. The prefix will not be inserted into the routing table as a Connected prefix. If the prefix is already present in the routing table as a Connected prefix (for example, because the prefix was also configured using the **ipv6 address** command), then it will be removed.
no-rtr-address	(Optional) Indicates that the router will not send the full router address in prefix advertisements and will not set the R bit.
no-autoconfig	(Optional) Indicates to hosts on the local link that the specified prefix cannot be used for IPv6 autoconfiguration. The prefix will be advertised with the A-bit clear.
no-onlink	(Optional) Configures the specified prefix as not on-link. The prefix will be advertised with the L-bit clear.
at *valid-date* *preferred-date*	(Optional) The date and time at which the lifetime and preference expire. The prefix is valid until this specified date and time are reached. Dates are expressed in the form *date-valid-expire month-valid-expire year-valid-expire* and *hh:mm-valid-expire date-prefer-expire month-prefer-expire year-valid-expire hh:mm-prefer-expire*.

Command Default

All prefixes configured on interfaces that originate IPv6 router advertisements are advertised with a valid lifetime of 2,592,000 seconds (30 days) and a preferred lifetime of 604,800 seconds (7 days).

Note that by default:

- All prefixes will be inserted in the routing table as Connected prefixes
- All prefixes will be advertised as on-link (for example, the L-bit will be set in the advertisement)
- All prefixes will be advertised as an autoconfiguration prefix (for example, the A-bit will be set in the advertisement)

Command Modes

Interface configuration

Command History

Release	Modification
12.2(13)T	This command was introduced. This command replaces the **ipv6 nd prefix-advertisement** command.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(11)T	The **no-rtr-address** 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.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(32.08.01)REC154	The **no-onlink** keyword was added.

Usage Guidelines

This command allows control over the individual parameters per prefix, including whether the prefix should be advertised.

By default, prefixes configured as addresses on an interface using the **ipv6 address** command are advertised in router advertisements. If you configure prefixes for advertisement using the **ipv6 nd prefix** command, then only these prefixes are advertised.

Default Parameters

The **default** keyword can be used to set default parameters for all prefixes.

Prefix Lifetime and Expiration

A date can be set to specify the expiration of a prefix. The valid and preferred lifetimes are counted down in real time. When the expiration date is reached, the prefix will no longer be advertised.

On-Link

When on-link is “on” (by default), the specified prefix is assigned to the link. Nodes sending traffic to such addresses that contain the specified prefix consider the destination to be locally reachable on the link.

Autoconfiguration

When autoconfiguration is “on” (by default), it indicates to hosts on the local link that the specified prefix can be used for IPv6 autoconfiguration.

The configuration options affect the L-bit and A-bit settings associated with the prefix in the IPv6 ND Router Advertisement, and presence of the prefix in the routing table, as follows:

- Default L=1 A=1 In Routing Table
- **no-onlink** L=0 A=1 In Routing Table

- **no-autoconfig** L=1 A=0 In Routing Table
- **no-onlink no-autoconfig** L=0 A=0 In Routing Table
- **off-link** L=0 A=1 Not in Routing Table
- **off-link no-autoconfig** L=0 A=0 Not in Routing Table

Examples

The following example includes the IPv6 prefix 2001:0DB8::/35 in router advertisements sent out Ethernet interface 0/0 with a valid lifetime of 1000 seconds and a preferred lifetime of 900 seconds:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 nd prefix 2001:0DB8::/35 1000 900
```

The following example advertises the prefix with the L-bit clear, so that the prefix is retained in the IPv6 routing table:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 address 2001::1/64
Router(config-if)# ipv6 nd prefix 2001::/64 3600 3600 no-onlink
```

Related Commands

Command	Description
ipv6 address link-local	Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface.
ipv6 address eui-64	Configures an IPv6 address and enables IPv6 processing on an interface using an EUI-64 interface ID in the low-order 64 bits of the address.
ipv6 mobile home-agent (interface configuration)	Initializes and starts the IPv6 Mobile home agent on a specific interface.
ipv6 nd managed-config-flag	Sets the “managed address configuration” flag in IPv6 router advertisements.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd prefix framed-ipv6-prefix

To add the prefix in a received RADIUS framed IPv6 prefix attribute to the interface's neighbor discovery prefix queue, use the **ipv6 nd prefix framed-ipv6-prefix** command in interface configuration mode. To disable this feature, use the **no** form of this command.

ipv6 nd prefix framed-ipv6-prefix

no ipv6 nd prefix framed-ipv6-prefix

Syntax Description

This command has no arguments or keywords.

Command Default

Prefix is sent in the router advertisements (RAs).

Command Modes

Interface 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 12.2(33)SRA.

Usage Guidelines

Use the **ipv6 nd prefix framed-ipv6-prefix** command to add the prefix in a received RADIUS framed IPv6 prefix attribute to the interface's neighbor discovery prefix queue and include it in RAs sent on the interface's link. By default, the prefix is sent in RAs. If the prefix in the attribute should be used by other applications such as the Dynamic Host Configuration Protocol (DHCP) for IPv6 server, administrators can disable the default behavior with the **no** form of the command.

Examples

The following example adds the prefix in a received RADIUS framed IPv6 prefix attribute to the interface's neighbor discovery prefix queue:

```
ipv6 nd prefix framed-ipv6-prefix
```

ipv6 nd prefix-advertisement

Note Effective with Cisco IOS Release 12.2(13)T, the **ipv6 nd prefix-advertisement** command is replaced by the **ipv6 nd prefix** command. See the **ipv6 nd prefix** command for more information.

To configure which IPv6 prefixes are included in IPv6 router advertisements, use the **ipv6 nd prefix-advertisement** command in interface configuration mode. To remove the prefixes, use the **no** form of this command.

ipv6 nd prefix-advertisement *ipv6-prefix*/*prefix-length valid-lifetime preferred-lifetime* [**onlink**] [**autoconfig**]

no ipv6 nd prefix-advertisement *ipv6-prefix*/*prefix-length*

Syntax Description

ipv6-prefix	The IPv6 network number to include in router advertisements. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/*prefix-length*	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
valid-lifetime	The amount of time (in seconds) that the specified IPv6 prefix is advertised as being valid.
preferred-lifetime	The amount of time (in seconds) that the specified IPv6 prefix is advertised as being preferred.
onlink	(Optional) Indicates that the specified prefix is assigned to the link. Nodes sending traffic to such addresses that contain the specified prefix consider the destination to be locally reachable on the link.
autoconfig	(Optional) Indicates to hosts on the local link that the specified prefix can be used for IPv6 autoconfiguration.

Command Default

All prefixes configured on interfaces that originate IPv6 router advertisements are advertised with a valid lifetime of 2592000 seconds (30 days) and a preferred lifetime of 604800 seconds (7 days), and with both the “onlink” and “autoconfig” flags set.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)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(13)T	This command was replaced by the **ipv6 nd prefix** command.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.

Usage Guidelines

By default, prefixes configured on an interface using the **ipv6 address** command are advertised with "onlink" and "autoconfiguration" flags set. If you configure prefixes for advertisement using the **ipv6 nd prefix-advertisement** command, then only these prefixes are advertised.

Examples

The following example includes the IPv6 prefix 2001:0DB8::/35 in router advertisements sent out Ethernet interface 0/0 with a valid lifetime of 1000 seconds, a preferred lifetime of 900 seconds, and both the "onlink" and "autoconfig" flags set:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 nd prefix-advertisement 2001:0DB8::/35 1000 900 onlink autoconfig
```

Related Commands

Command	Description
ipv6 address link-local	Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface.
ipv6 address eui-64	Configures an IPv6 address and enables IPv6 processing on an interface using an EUI-64 interface ID in the low-order 64 bits of the address.
ipv6 nd managed-config-flag	Sets the "managed address configuration" flag in IPv6 router advertisements.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd ra interval

To configure the interval between IPv6 router advertisement (RA) transmissions on an interface, use the **ipv6 nd ra interval** command in interface configuration mode. To restore the default interval, use the **no** form of this command.

ipv6 nd ra interval {*maximum-secs* [*minimum-secs*] | **msec** *maximum-ms* [*minimum-ms*]}

no ipv6 nd ra interval

Syntax Description

maximum-secs	Maximum interval between IPv6 RA transmissions in seconds.
minimum-secs	(Optional) Minimum interval between IPv6 RA transmissions in seconds. The range is from 3 to 150.
msec	Intervals specified in milliseconds.
maximum-ms	Maximum interval between IPv6 RA transmissions in milliseconds.
minimum-ms	(Optional) Minimum interval between IPv6 RA transmissions in milliseconds. The smallest possible minimum RA interval is 30 milliseconds.

Command Default

The default is 200 seconds.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(2)T	This command was introduced. This command replaces the **ipv6 nd ra-interval** command.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
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.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

The interval between transmissions should be less than or equal to the IPv6 router advertisement lifetime if you configure the route as a default router by using the **ipv6 nd ra lifetime** command. To prevent synchronization with other IPv6 nodes, the actual interval used is randomly selected from a value between the minimum and maximum values.

Users can explicitly configure a minimum RA interval. The minimum RA interval may never be more than 75% of the maximum RA interval and never less than 3 seconds (if specified in seconds). If the minimum RA interval is not configured, then it is calculated as 75% of the maximum RA interval.

If the user specifies the time in milliseconds, then the smallest minimum RA interval is 30 milliseconds. This limit allows configuration of very short RA intervals for Mobile IPv6.

Examples

The following example configures an IPv6 router advertisement interval of 201 seconds for Ethernet interface 0/0:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 nd ra interval 201
```

The following examples shows a maximum RA interval of 200 seconds and a minimum RA interval of 50 seconds:

```
Router(config-if) ipv6 nd ra interval 200 50
```

The following examples shoes a maximum RA interval of 100 seconds and a minimum RA interval of 30 milliseconds, which is the smallest value allowed:

```
Router(config-if) ipv6 nd ra interval msec 100 30
```

Related Commands

Command	Description
ipv6 mobile home-agent (interface configuration)	Initializes and starts the Mobile IPv6 home agent on a specific interface.
ipv6 nd advertisement-interval	Configures the advertisement interval option to be sent in RAs.
ipv6 nd ra lifetime	Configures the router lifetime value in IPv6 router advertisements on an interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd ra lifetime

To configure the router lifetime value in IPv6 router advertisements on an interface, use the **ipv6 nd ra lifetime** command in interface configuration mode. To restore the default lifetime, use the **no** form of this command.

ipv6 nd ra lifetime *seconds*

no ipv6 nd ra lifetime

Syntax Description

seconds	The validity of this router as a default router on this interface (in seconds).

Command Default

The default lifetime value is 1800 seconds.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(2)T	This command was introduced. This command replaces the **ipv6 nd ra-lifetime** command.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
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.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

The "router lifetime" value is included in all IPv6 router advertisements sent out the interface. The value indicates the usefulness of the router as a default router on this interface. Setting the value to 0 indicates that the router should not be considered a default router on this interface. The "router lifetime" value can be set to a non zero value to indicate that it should be considered a default router on this interface. The non zero value for the "router lifetime" value should not be less than the router advertisement interval.

Examples

The following example configures an IPv6 router advertisement lifetime of 1801 seconds for Ethernet interface 0/0:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 nd ra lifetime 1801
```

Related Commands

Command	Description
ipv6 nd ra interval	Configures the interval between IPv6 router advertisement transmissions on an interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd ra suppress

To suppress IPv6 router advertisement transmissions on a LAN interface, use the **ipv6 nd ra suppress** command in interface configuration mode. To reenable the sending of IPv6 router advertisement transmissions on a LAN interface, use the **no** form of this command.

ipv6 nd ra suppress [**all**]

no ipv6 nd ra suppress

Syntax Description

all	(Optional) Suppresses all router advertisements (RAs) on an interface.

Command Default

IPv6 router advertisements are automatically sent on Ethernet and FDDI interfaces if IPv6 unicast routing is enabled on the interfaces. IPv6 router advertisements are not sent on other types of interfaces.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(2)T	This command was introduced. This command replaces the **ipv6 nd suppress-ra** command.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
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.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

The **ipv6 nd ra suppress** command only suppresses periodic unsolicited RAs. It does not suppress RAs sent in response to a router solicitation. To suppress all RAs, including those sent in response to a router solicitation, use the **ipv6 nd ra suppress** command with the **all** keyword.

Use the **no ipv6 nd ra suppress** command to enable the sending of IPv6 RA transmissions on non-LAN interface types (for example, serial or tunnel interfaces).

Examples

The following example suppresses IPv6 router advertisements on Ethernet interface 0/0:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 nd ra suppress
```

The following example enables the sending of IPv6 router advertisements on serial interface 0/1:

```
Router(config)# interface serial 0/1
Router(config-if)# no ipv6 nd ra suppress
```

Related Commands

Command	Description
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd ra-interval

Note Effective with Cisco IOS Release 12.4(2)T, the **ipv6 nd ra-interval** command is replaced by the **ipv6 nd ra interval** command. See the **ipv6 nd ra interval** command for more information.

To configure the interval between IPv6 router advertisement (RA) transmissions on an interface, use the **ipv6 nd ra-interval** command in interface configuration mode. To restore the default interval, use the **no** form of this command.

ipv6 nd ra-interval {*seconds* | **msec** *milliseconds*}

no ipv6 nd ra-interval

Syntax Description

seconds	Interval between IPv6 RA transmissions in seconds.
msec	Allows specification of interval between IPv6 RA transmissions in milliseconds.
milliseconds	Interval between IPv6 RA transmissions in milliseconds.

Command Default

The default is 200 seconds.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)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 Release 12.2(14)S.
12.3(14)T	The **msec** keyword and *milliseconds* argument were added.
12.4(2)T	This command was replaced by the **ipv6 nd ra interval** command.

Usage Guidelines

The interval between transmissions should be less than or equal to the IPv6 router advertisement lifetime if you configure the route as a default router by using the **ipv6 nd ra-lifetime** command. To prevent synchronization with other IPv6 nodes, randomly adjust the actual value used to within 20 percent of the specified value.

The **msec** keyword along with the *milliseconds* argument allow the RA interval to be set to a low value to aid movement detection by a mobile node.

Examples

The following example configures an IPv6 router advertisement interval of 201 seconds for Ethernet interface 0/0:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 nd ra-interval 201
```

Related Commands

Command	Description
ipv6 mobile home-agent (interface configuration)	Initializes and starts the Mobile IPv6 home agent on a specific interface.
ipv6 nd advertisement-interval	Configures the advertisement interval option to be sent in RAs.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd ra-lifetime

Note Effective with Cisco IOS Release 12.4(2)T, the **ipv6 nd ra-lifetime** command is replaced by the **ipv6 nd ra lifetime** command. See the **ipv6 nd ra lifetime** command for more information.

To configure the "router lifetime" value in IPv6 router advertisements on an interface, use the **ipv6 nd ra-lifetime** command in interface configuration mode. To restore the default lifetime, use the **no** form of this command.

ipv6 nd ra-lifetime *seconds*

no ipv6 nd ra-lifetime

Syntax Description

seconds	The validity of this router as a default router on this interface (in seconds).

Command Default

The default is 1800 seconds.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)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 Release 12.2(14)S.
12.4(2)T	This command was replaced by the **ipv6 nd ra lifetime** command.

Usage Guidelines

The "router lifetime" value is included in all IPv6 router advertisements sent out the interface. The value indicates the usefulness of the router as a default router on this interface. Setting the value to 0 indicates that the router should not be considered a default router on this interface. The "router lifetime" value can be set to a nonzero value to indicate that it should be considered a default router on this interface. The nonzero value for the "router lifetime" value should not be less than the router advertisement interval.

Examples

The following example configures an IPv6 router advertisement lifetime of 1801 seconds for Ethernet interface 0/0:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 nd ra-lifetime 1801
```

Related Commands

Command	Description
ipv6 nd ra-interval	Configures the interval between IPv6 router advertisement transmissions on an interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd raguard

To apply the router advertisements (RA) guard feature, use the **ipv6 nd raguard** command in interface configuration mode.

ipv6 nd raguard

no ipv6 nd raguard

Syntax Description

This command has no arguments or keywords.

Command Default

An RA guard policy is not configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI4	This command was introduced.
12.2(54)SG	This command was modified. Support for Cisco IOS Release 12.2(54)SG was added.

Usage Guidelines

The **ipv6 nd raguard** command enables the RA guard feature. If the RA does not match with the configured option, the packet is dropped.

Examples

The following example applies the RA guard:

```
Router(config-if)# ipv6 nd raguard
```

ipv6 nd raguard attach-policy

To apply the router advertisement (RA) guard feature on a specified interface, use the **ipv6 nd raguard attach-policy** command in interface configuration mode.

ipv6 nd raguard attach-policy [*policy-name* [**vlan** {**add** | **except** | **none** | **remove** | **all**} *vlan* [*vlan1, vlan2, vlan3...*]]]

Syntax Description

policy-name	(Optional) RA guard policy name.
vlan	(Optional) Applies the RA guard feature to a VLAN on the interface.
add	Adds a VLAN to be inspected.
except	All VLANs are inspected except the one specified.
none	No VLANs are inspected.
remove	Removes the specified VLAN from RA guard inspection.
all	ND traffic from all VLANs on the port is inspected.
vlan	(Optional) A specific VLAN on the interface. More than one VLAN can be specified (*vlan1*, *vlan2*, *vlan3...*). The VLAN number that can be used is from 1 through 4094.

Command Default

An RA guard policy is not configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

If no policy is specified using the *policy-name* argument, the port device role is set to host and all inbound router traffic (e.g., RA and redirect messages) is blocked.

If no VLAN is specified (which is equal to entering the **vlan all** keywords after the *policy-name* argument), RA guard traffic from all VLANs on the port is analyzed.

If specified. the VLAN parameter is either a single VLAN number from 1 through 4094 or a range of VLANs described by two VLAN numbers, the lesser one first, separated by a dash. Do not enter any spaces between comma-separated vlan parameters or in dash-specified ranges; for example, vlan 1-100,200,300-400.

Examples

In the following example, the RA guard feature is applied on the GigabitEthernet 0/0 interface:

```
Router(config)# interface GigabitEthernet 0/0
Router(config-if)# ipv6 nd raguard attach-policy
```

ipv6 nd raguard policy

To define the router advertisement (RA) guard policy name and enter RA guard policy configuration mode, use the **ipv6 nd raguard policy** command in global configuration mode.

ipv6 nd raguard policy *policy-name*

Syntax Description

policy-name	IPv6 RA guard policy name.

Command Default

An RA guard policy is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

Use the **ipv6 nd raguard policy** command to configure RA guard globally on a router.

Once you are in ND inspection policy configuration mode, you can use any of the following subcommands:

- **device-role**
- **drop-unsecure**
- **limit address-count**
- **sec-level minimum**
- **trusted-port**
- **validate source-mac**

After IPv6 RA guard is configured globally, you can use the **ipv6 nd raguard attach-policy** command to enable IPv6 RA guard on a specific interface.

Examples

The following example defines the RA guard policy name as policy1 and enters the router into policy configuration mode:

```
Router(config)# ipv6 nd raguard policy policy1
Router(config-ra-guard)#
```

Related Commands

Command	Description
device-role	Specifies the role of the device attached to the port.
drop-unsecure	Drops messages with no or invalid options or an invalid signature.

Command	Description
ipv6 nd raguard attach-policy	Applies the IPv6 RA guard feature on a specified interface.
limit address-count	Limits the number of IPv6 addresses allowed to be used on the port.
sec-level minimum	Specifies the minimum security level parameter value when CGA options are used.
trusted-port	Configures a port to become a trusted port.
validate source-mac	Checks the source MAC address against the link-layer address.

ipv6 nd reachable-time

To configure the amount of time that a remote IPv6 node is considered reachable after some reachability confirmation event has occurred, use the **ipv6 nd reachable-time** command in interface configuration mode. To restore the default time, use the **no** form of this command.

ipv6 nd reachable-time *milliseconds*

no ipv6 nd reachable-time

Syntax Description

milliseconds	The amount of time that a remote IPv6 node is considered reachable (in milliseconds).

Command Default

0 milliseconds (unspecified) is advertised in router advertisements and the value 30000 (30 seconds) is used for the neighbor discovery activity of the router itself.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)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 Release 12.2(14)S.
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.
12.2(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 configured time enables the router to detect unavailable neighbors. Shorter configured times enable the router to detect unavailable neighbors more quickly; however, shorter times consume more IPv6 network bandwidth and processing resources in all IPv6 network devices. Very short configured times are not recommended in normal IPv6 operation.

The configured time is included in all router advertisements sent out of an interface so that nodes on the same link use the same time value. A value of 0 means indicates that the configured time is unspecified by this router.

Examples

The following example configures an IPv6 reachable time of 1,700,000 milliseconds for Ethernet interface 0/0:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 nd reachable-time 1700000
```

Related Commands

Command	Description
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd resolution data limit

To configure the number of data packets queued pending Neighbor Discovery resolution, use the **ipv6 nd resolution data limit** command in global configuration mode.

ipv6 nd resolution data limit *number-of-packets*

no ipv6 nd resolution data limit *number-of-packets*

Syntax Description

number-of-packets	The number of queued data packets. The range is from 16 to 2048 packets.

Command Default

Queue limit is 16 packets.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.

Usage Guidelines

The **ipv6 nd resolution data limit** command allows the customer to configure the number of data packets queued pending Neighbor Discovery resolution. IPv6 Neighbor Discovery queues a data packet that initiates resolution for an unresolved destination. Neighbor Discovery will only queue one packet per destination. Neighbor Discovery also enforces a global (per-router) limit on the number of packets queued. Once the global queue limit is reached, further packets to unresolved destinations are discarded. The minimum (and default) value is 16 packets, and the maximum value is 2048.

In most situations, the default value of 16 queued packets pending Neighbor Discovery resolution is sufficient. However, in some high-scalability scenarios in which the router needs to initiate communication with a very large number of neighbors almost simultaneously, then the value may be insufficient. This may lead to loss of the initial packet sent to some neighbors. In most applications, the initial packet is retransmitted, so initial packet loss generally is not a cause for concern. (Note that dropping the initial packet to an unresolved destination is normal in IPv4.) However, there may be some high-scale configurations where loss of the initial packet is inconvenient. In these cases, the customer can use the **ipv6 nd resolution data limit** command to prevent the initial packet loss by increasing the unresolved packet queue size.

Examples

The following example configures the global number of data packets held awaiting resolution to be 32:

```
Router(config)# ipv6 nd resolution data limit 32
```

ipv6 nd router-preference

To configure a default router preference (DRP) for the router on a specific interface, use the **ipv6 nd router-preference** command in interface configuration mode. To return to the default DRP, use the **no** form of this command.

ipv6 nd router-preference {**high** | **medium** | **low**}

no ipv6 nd router-preference

Syntax Description

high	Preference for the router specified on an interface is high.
medium	Preference for the router specified on an interface is medium.
low	Preference for the router specified on an interface is low.

Command Default

Router advertisements (RAs) are sent with the **medium** preference.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

RA messages are sent with the DRP configured by the **ipv6 nd router-preference** command. If no DRP is configured, RAs are sent with a medium preference.

A DRP is useful when, for example, two routers on a link may provide equivalent, but not equal-cost, routing, and policy may dictate that hosts should prefer one of the routers.

Examples

The following example configures a DRP of high for the router on gigabit Ethernet interface 0/1:

```
Router(config)# interface Gigabit ethernet 0/1
Router(config-if)# ipv6 nd router-preference high
```

Related Commands

Command	Description
ipv6 nd ra interval	Configures the interval between IPv6 router advertisement transmissions on an interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd secured certificate-db

To configure the maximum number of entries in an IPv6 Secure Neighbor Discovery (SeND) certificate database, use the **ipv6 nd secured certificate-db** command in global configuration mode. To disable any maximum number of entries set for a SeND certificate database, use the **no** form of this command.

ipv6 nd secured certificate-db max-entries *max-entries-value*

no ipv6 nd secured certificate-db max-entries

Syntax Description

max-entries *max-entries-value*	Specifies the maximum number of entries in the certificate database. The range is from 1 to 1000.

Command Default

No SeND certificate database is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

This command allows you to set up a maximum size for the certificate database (DB), to protect against denial of service (DoS) certificate flooding. When the limit is reached, new certificates are dropped.

The certificate DB is relevant on a router in host mode only, because it stores certificates received from routers.

Examples

The following example configures a SeND certificate database with a maximum number of 500 entries:

```
Router(config)# ipv6 nd secured certificate-db max-entries 500
```

Related Commands

Command	Description
ipv6 nd secured full-secure (global configuration)	Enables SeND security mode on a router.
ipv6 nd secured full-secure (interface configuration)	Enables SeND security mode on a specified interface.
ipv6 nd secured key-length	Configures SeND key-length options.
ipv6 nd secured timestamp	Configures the SeND time stamp.
ipv6 nd secured timestamp-db	Configures the maximum number of entries that did not reach the destination in a SeND time-stamp database.

ipv6 nd secured full-secure

To enable the secure mode for IPv6 Secure Neighbor Discovery (SeND) on a router, use the **ipv6 nd secured full-secure** command in global configuration mode. To disable SeND security mode, use the **no** form of this command.

ipv6 nd secured full-secure

no ipv6 nd secured full-secure

Syntax Description

This command has no arguments or keywords.

Command Default

Non-SeND neighbor discovery messages are accepted by the router.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

The **ipv6 nd secured full-secure** command in global configuration mode allows you to configure the router to accept or reject non-SeND neighbor discovery messages. If this command is enabled, non-SeND messages are rejected by the specified router.

Examples

The following example enables SeND security mode on a router:

```
Router(config)# ipv6 nd secured full-secure
```

Related Commands

Command	Description
ipv6 nd secured full-secure (interface configuration)	Enables SeND security mode on a specified interface.

ipv6 nd secured full-secure (interface)

To enable the secure mode for IPv6 Secure Neighbor Discovery (SeND) on a specified interface, use the **ipv6 nd secured full-secure** command in interface configuration mode. To provide the co-existence mode for secure and nonsecure neighbor discovery messages on an interface, use the **no** form of this command.

ipv6 nd secured full-secure

no ipv6 nd secured full-secure

Syntax Description

This command has no arguments or keywords.

Command Default

Non-SeND messages are accepted by the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

The **ipv6 nd secured full-secure** command in interface configuration mode allows you to configure a specified interface to accept or reject non-SeND neighbor discovery messages. If this command is enabled, non-SeND messages are rejected by the interface. If this command is not enabled, secure and nonsecure neighbor discovery messages can coexist on the same interface.

Examples

The following example enables SeND security mode on an interface:

```
Router(config)# interface Ethernet0/0
Router(config-if)# ipv6 nd secured full-secure
```

Related Commands

Command	Description
ipv6 nd secured full-secure (global configuration)	Enables SeND security mode on a specified router.

ipv6 nd secured key-length

To configure IPv6 Secure Neighbor Discovery (SeND) key-length options, use the **ipv6 nd secured key-length** command in global configuration mode. To disable the key length, use the **no** form of this command.

ipv6 nd secured key-length [[**minimum** | **maximum**] *value*]

no ipv6 nd secured key-length

Syntax Description

minimum *value*	(Optional) Sets the minimum key-length value, which should be at least 384 bits. The range is from 384 to 2048 bits, and the default key-length value is 1024 bits.
maximum *value*	(Optional) Sets the maximum key-length value. The range is from 384 to 2048 bits, and the default key-length value is 1024 bits.

Command Default

The key length is 1024 bits.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

When used by SeND, the key length is checked against the key-length value, as set in the **ipv6 nd secured key-length** command. When packets are received from a neighbor with a key length that is out of the configured boundaries, the packets are treated as unsecure.

Examples

The following example sets the minimum key-length value to 512 bits and the maximum value to 1024 bits:

```
Router(config)# ipv6 nd secured key-length minimum 512
Router(config)# ipv6 nd secured key-length maximum 1024
```

Related Commands

Command	Description
ipv6 nd secured certificate-db	Configures the maximum number of entries in a SeND certificate database.
ipv6 nd secured full-secure (global configuration)	Enables SeND security mode on a specified router.
ipv6 nd secured full-secure (interface configuration)	Enables SeND security mode on a specified interface.

Command	Description
ipv6 nd secured timestamp	Configures the SeND time stamp.
ipv6 nd secured timestamp-db	Configures the maximum number of entries in a SeND time-stamp database.

ipv6 nd secured sec-level

To configure the minimum security value that IPv6 Secure Neighbor Discovery (SeND) will accept from its peer, use the **ipv6 nd secured sec-level** command in global configuration mode. To disable the security level, use the **no** form of this command.

ipv6 nd secured sec-level [**minimum** *value*]

no ipv6 nd secured sec-level

Syntax Description

minimum *value*	(Optional) Sets the minimum security level, which is a value from 0 through 3. The default security level is 1. The most secure level is 3.

Command Default

The default security level is 1.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

The **ipv6 nd secured sec-level** command allows the user to configure the minimum security value the router will accept from its peer.

Examples

The following example sets the minimum security level to 2:

```
Router(config)# ipv6 nd secured sec-level 2
```

Related Commands

Command	Description
ipv6 nd secured certificate-db	Configures the maximum number of entries in a SeND certificate database.
ipv6 nd secured full-secure (global configuration)	Enables SeND security mode on a specified router.
ipv6 nd secured full-secure (interface configuration)	Enables SeND security mode on a specified interface.
ipv6 nd secured key-length	Configures SeND key-length options.
ipv6 nd secured timestamp	Configures the SeND time stamp.
ipv6 nd secured timestamp-db	Configures the maximum number of unreached entries in a SeND time-stamp database.

ipv6 nd secured timestamp

To configure the IPv6 Secure Neighbor Discovery (SeND) time stamp, use the **ipv6 nd secured timestamp** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

ipv6 nd secured timestamp {**delta** *value* | **fuzz** *value*}

no ipv6 nd secured timestamp

Syntax Description

delta *value*	Specifies the maximum time difference accepted between the sender and the receiver. Default value is 300 seconds.
fuzz *value*	Specifies the maximum age of the message, when the delta is taken into consideration; that is, the amount of time, in seconds, that a packet can arrive after the delta value before being rejected. Default value is 1 second.

Command Default

Default time-stamp values are used.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

The **ipv6 nd secured timestamp** command configures the amount of time the router waits before it accepts or rejects packets it has received.

Examples

The following example configures the SeND time stamp to be 600 seconds:

```
Router(config)# interface Ethernet0/0
Router(config-if)# ipv6 nd secured timestamp delta 600
```

Related Commands

Command	Description
ipv6 nd secured certificate-db	Configures the maximum number of entries in a SeND certificate database.
ipv6 nd secured full-secure (global configuration)	Enables SeND security mode on a specified router.
ipv6 nd secured full-secure (interface configuration)	Enables SeND security mode on a specified interface.
ipv6 nd secured key-length	Configures SeND key-length options.
ipv6 nd secured timestamp-db	Configures the maximum number of unreached entries in a SeND time-stamp database.

ipv6 nd secured timestamp-db

To configure the maximum number of unreached entries in an IPv6 Secure Neighbor Discovery (SeND) time-stamp database, use the **ipv6 nd secured timestamp-db** command in global configuration mode. To return to the default settings, use the **no** form of this command.

ipv6 nd secured timestamp-db max-entries *max-entries-value*

no ipv6 nd secured timestamp-db max-entries

Syntax Description

max-entries *max-entries-value*	Specifies the maximum number of entries in the certificate database. The range is from 1 to 1000.

Command Default

No time-stamp database is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Examples

The following example configures the time-stamp database on a router:

```
Router(config)# ipv6 nd secured timestamp-db max-entries 345
```

Related Commands

Command	Description
ipv6 nd secured certificate-db	Configures the maximum number of entries in a SeND certificate database.
ipv6 nd secured full-secure (global configuration)	Enables SeND security mode on a specified router.
ipv6 nd secured full-secure (interface configuration)	Enables SeND security mode on a specified interface.
ipv6 nd secured key-length	Configures SeND key-length options.
ipv6 nd secured timestamp	Configures the SeND time stamp.

ipv6 nd secured trustanchor

To specify an IPv6 Secure Neighbor Discovery (SeND) trusted anchor on an interface, use the **ipv6 nd secured trustanchor** command in interface configuration mode. To remove a trusted anchor, use the **no** form of this command.

ipv6 nd secured trustanchor *trustanchor-name*

no ipv6 nd secured trustanchor *trustanchor-name*

Syntax Description

trustanchor-name	The name to be found in the certificate of the trustpoint.

Command Default

No trusted anchor is defined.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

The **ipv6 nd secured trustanchor** command is used to select the certificate authority (CA) you want to authenticate. The trusted anchors configured by this command act as references to the trustpoints configured.

A crypto Public Key Infrastructure (PKI) trustpoint can be a self-signed root CA or a subordinate CA. The *trustpoint-name* argument refers to the name to be found in the certificate of the trustpoint.

The **ipv6 nd secured trustanchor** and **ipv6 nd secured trustpoint** commands both generate an entry in the SeND configuration database that points to the trustpoint provided. More than one trustpoint can be provided for each command, and the same trustpoint can be used in both commands.

Examples

The following example specifies trusted anchor anchor1 on Ethernet interface 0/0:

```
Router(config)# interface Ethernet0/0
Router(config-if)# ipv6 nd secured trustanchor anchor1
```

Related Commands

Command	Description
crypto pki trustpoint	Declares the trustpoint that your router should use.
ipv6 nd secured trustpoint	Specifies which trustpoint should be used for selecting the certificate to advertise.

ipv6 nd secured trustpoint

To specify which trustpoint should be used in the ipv6 Secure Neighbor Discovery (SeND) protocol for selecting the certificate to advertise, use the **ipv6 nd secured trustpoint** command in interface configuration mode. To disable the trustpoint, use the **no** form of this command.

ipv6 nd secured trustpoint *trustpoint-name*

no ipv6 nd secured trustpoint *trustpoint-name*

Syntax Description

trustpoint-name	The name to be found in the certificate of the trustpoint.

Command Default

SeND is not enabled on a specified interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

The **ipv6 nd secured trustpoint** command enables SeND on an interface and specifies which trustpoint should be used. The trustpoint points to the Rivest, Shamir, and Adelman (RSA) key pair and the trusted anchor (which is the certificate authority [CA] signing your certificate).

The **ipv6 nd secured trustpoint** and **ipv6 nd secured trustanchor** commands both generate an entry in the SeND configuration database that points to the trustpoint provided. More than one trustpoint can be provided for each command, and the same trustpoint can be used in both commands. However, the trustpoint provided in the **ipv6 nd secured trustpoint** command must include a router certificate and the signing CA certificate. It may also include the certificate chain up to the root certificate provided by a CA that hosts (connected to the router) will trust.

The trustpoint provided in the **ipv6 nd secured trustanchor** command must only include a CA certificate.

Examples

The following example specifies trusted anchor anchor1 on Ethernet interface 0/0:

```
Router(config)# interface Ethernet0/0
Router(config-if)# ipv6 nd secured trustpoint trustpoint1
```

Related Commands

Command	Description
crypto pki trustpoint	Declares the trustpoint that your router should use.
ipv6 nd secured trustanchor	Specifies a trusted anchor on an interface.

ipv6 nd suppress-ra

Note Effective with Cisco IOS Release 12.4(2)T, the **ipv6 nd suppress-ra** command is replaced by the **ipv6 nd ra suppress** command. See the **ipv6 nd ra suppress** command for more information.

To suppress IPv6 router advertisement transmissions on a LAN interface, use the **ipv6 nd suppress-ra** command in interface configuration mode. To reenable the sending of IPv6 router advertisement transmissions on a LAN interface, use the **no** form of this command.

ipv6 nd suppress-ra

no ipv6 nd suppress-ra

Syntax Description

This command has no arguments or keywords.

Command Default

IPv6 router advertisements are automatically sent on Ethernet and FDDI interfaces if IPv6 unicast routing is enabled on the interfaces. IPv6 router advertisements are not sent on other types of interfaces.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)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 Release 12.2(14)S.
12.4(2)T	This command was replaced by the **ipv6 nd ra suppress** command.

Usage Guidelines

Use the **no ipv6 nd suppress-ra** command to enable the sending of IPv6 router advertisement transmissions on non-LAN interface types (for example, serial or tunnel interfaces).

Examples

The following example suppresses IPv6 router advertisements on Ethernet interface 0/0:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 nd suppress-ra
```

The following example enables the sending of IPv6 router advertisements on serial interface 0/1:

```
Router(config)# interface serial 0/1
Router(config-if)# no ipv6 nd suppress-ra
```

Related Commands

Command	Description
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 neighbor

To configure a static entry in the IPv6 neighbor discovery cache, use the **ipv6 neighbor** command in global configuration mode. To remove a static IPv6 entry from the IPv6 neighbor discovery cache, use the **no** form of this command.

ipv6 neighbor *ipv6-address interface-type interface-number hardware-address*

no ipv6 neighbor *ipv6-address interface-type interface-number*

Syntax Description

ipv6-address	The IPv6 address that corresponds to the local data-link address. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
interface-type	The specified interface type. For supported interface types, use the question mark (?) online help function.
interface-number	The specified interface number.
hardware-address	The local data-link address (a 48-bit address).

Command Default

Static entries are not configured in the IPv6 neighbor discovery cache.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)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 Release 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.

Usage Guidelines

The **ipv6 neighbor** command is similar to the **arp** (global) command.

If an entry for the specified IPv6 address already exists in the neighbor discovery cache—learned through the IPv6 neighbor discovery process—the entry is automatically converted to a static entry.

Use the **show ipv6 neighbors** command to view static entries in the IPv6 neighbor discovery cache. A static entry in the IPv6 neighbor discovery cache can have one of the following states:

- INCMP (Incomplete)—The interface for this entry is down.
- REACH (Reachable)—The interface for this entry is up.

Note Reachability detection is not applied to static entries in the IPv6 neighbor discovery cache; therefore, the descriptions for the INCMP and REACH states are different for dynamic and static cache entries. See the **show ipv6 neighbors** command for descriptions of the INCMP and REACH states for dynamic cache entries.

The **clear ipv6 neighbors** command deletes all entries in the IPv6 neighbor discovery cache, except static entries. The **no ipv6 neighbor** command deletes a specified static entry from the neighbor discovery cache; the command does not remove dynamic entries—learned from the IPv6 neighbor discovery process—from the cache. Disabling IPv6 on an interface by using the **no ipv6 enable** command or the **no ipv6 unnumbered** command deletes all IPv6 neighbor discovery cache entries configured for that interface, except static entries (the state of the entry changes to INCMP).

Static entries in the IPv6 neighbor discovery cache are not modified by the neighbor discovery process.

Note Static entries for IPv6 neighbors can be configured only on IPv6-enabled LAN and ATM LAN Emulation interfaces.

Examples

The following example configures a static entry in the IPv6 neighbor discovery cache for a neighbor with the IPv6 address 2001:0DB8::45A and link-layer address 0002.7D1A.9472 on Ethernet interface 1:

```
Router(config)# ipv6 neighbor 2001:0DB8::45A ethernet1 0002.7D1A.9472
```

Related Commands

Command	Description
arp (global)	Adds a permanent entry in the ARP cache.
clear ipv6 neighbors	Deletes all entries in the IPv6 neighbor discovery cache, except static entries.
no ipv6 enable	Disables IPv6 processing on an interface that has not been configured with an explicit IPv6 address.
no ipv6 unnumbered	Disables IPv6 on an unnumbered interface.
show ipv6 neighbors	Displays IPv6 neighbor discovery cache information.

ipv6 neighbor binding

To change the defaults of neighbor binding entries in a binding table, use the **ipv6 neighbor binding** command in global configuration mode. To return the networking device to its default, use the **no** form of this command.

ipv6 neighbor binding [**reachable-lifetime** *value* | **stale-lifetime** *value*]

no ipv6 neighbor binding

Syntax Description

reachable-lifetime *value*	(Optional) The maximum time, in seconds, an entry is considered reachable without getting a proof of reachability (direct reachability through tracking, or indirect reachability through Neighbor Discovery protocol [NDP] inspection). After that, the entry is moved to stale. The range is from 1 through 3600 seconds, and the default is 300 seconds (or 5 minutes).
stale-lifetime *value*	(Optional) The maximum time, in seconds, a stale entry is kept in the binding table before the entry is deleted or proof is received that the entry is reachable. • The default is 24 hours (86,400 seconds).
down-lifetime *value*	(Optional) The maximum time, in seconds, an entry learned from a down interface is kept in the binding table before the entry is deleted or proof is received that the entry is reachable. • The default is 24 hours (86,400 seconds).

Command Default

Reachable lifetime: 300 seconds
Stale lifetime: 24 hours
Down lifetime: 24 hours

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

Use the **ipv6 neighbor binding** command to configure information about individual entries in a binding table. If no keywords or arguments are configured, the IPv6 neighbor binding entry defaults are used.

If the **tracking reachable-lifetime** command is configured, it overrides **ipv6 neighbor binding reachable-lifetime** configuration. If the **tracking stale-lifetime** command is configured, it overrides **ipv6 neighbor binding stale-lifetime** configuration.

Examples

The following example shows how to change the reachable lifetime for binding entries to 100 seconds:

```
Router(config)# ipv6 neighbor binding reachable-entries 100
```

Related Commands

Command	Description
ipv6 neighbor tracking	Tracks entries in the binding table.
tracking	Overrides the default tracking policy on a port.

ipv6 neighbor binding down-lifetime

To change the default of a neighbor binding entry's down lifetime, use the **ipv6 neighbor binding down-lifetime** command in global configuration mode. To return the networking device to its default, use the **no** form of this command.

ipv6 neighbor binding down-lifetime {*value* | **infinite**}

no ipv6 neighbor binding down-lifetime

Syntax Description

value	The maximum time, in minutes, an entry learned from a down interface is kept in the table before deletion. The range is from 1 to 3600 minutes. • The default is 24 hours (86,400 seconds).
infinite	Keeps an entry in the binding table for an infinite amount of time.

Command Default

A neighbor binding entry is down for 24 hours before it is deleted from the binding table.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

Use the **ipv6 neighbor binding down-lifetime** command to change the amount of time a neighbor binding is down before that binding is removed from the binding table.

Examples

The following example shows how to change a binding entry's down lifetime to 2 minutes before it is deleted from the binding table:

```
Router(config)# ipv6 neighbor binding down-lifetime 2
```

Related Commands

Command	Description
ipv6 neighbor tracking	Tracks entries in the binding table.

ipv6 neighbor binding logging

To enable the logging of binding table main events, use the **ipv6 neighbor binding logging** command in global configuration mode. To disable this feature, use the **no** form of this command.

ipv6 neighbor binding logging

no ipv6 neighbor binding logging

Syntax Description

This command has no arguments or keywords.

Command Default

Binding table events are not logged.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

The **ipv6 neighbor binding logging** command enables the logging of the following binding table events:

- An entry is inserted into the binding table.
- A binding table entry was updated.
- A binding table entry was deleted from the binding table.
- A binding table entry was not inserted into the binding table, possibly because of a collision with an existing entry, or because the maximum number of entries has been reached.

Examples

The following example shows how to enable binding table event logging:

```
Router(config)# ipv6 neighbor binding logging
```

Related Commands

Command	Description
ipv6 neighbor binding vlan	Adds a static entry to the binding table database.
ipv6 neighbor tracking	Tracks entries in the binding table.
ipv6 snooping logging packet drop	Configures IPv6 snooping security logging.

ipv6 neighbor binding max-entries

To specify the maximum number of entries that are allowed to be inserted in the binding table cache, use the **ipv6 neighbor binding max-entries** command in global configuration mode. To return to the default number of entries, use the **no** form of this command.

ipv6 neighbor binding max-entries *entries* [**vlan-limit** *number* | **interface-limit** *number* | **mac-limit** *number*]

no ipv6 neighbor binding max-entries *entries* [**vlan-limit** | **mac-limit**]

Syntax Description

entries	Number of entries that can be inserted into the cache.
vlan-limit *number*	(Optional) Specifies a neighbor binding limit per number of VLANs.
interface-limit *number*	(Optional) Specifies a neighbor binding limit per interface.
mac-limit *number*	(Optional) Specifies a neighbor binding limit per number of Media Access Control (MAC) addresses.

Command Default

This command is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

The **ipv6 neighbor binding max-entries** command is used to control the content of the binding table. This command specifies the maximum number of entries that are allowed to be inserted in the binding table cache. Once this limit is reached, new entries are refused, and the Neighbor Discovery Protocol (NDP) traffic source with the new entry is dropped.

If the maximum number of entries specified is lower than the current number of entries in database, no entries are cleared, and the new threshold is reached after normal cache attrition.

The maximum number of entries limit can be set globally, by number of VLANs, or by number of MAC addresses.

Examples

The following example shows how to specify globally the maximum number of entries inserted into the cache:

```
Router(config)# ipv6 neighbor binding max-entries
```

Related Commands

Command	Description
ipv6 neighbor binding vlan	Adds a static entry to the binding table database.
ipv6 neighbor tracking	Tracks entries in the binding table.

ipv6 neighbor binding stale-lifetime

To set the length of time a stale entry is kept in the binding table, use the **ipv6 neighbor binding stale-lifetime** command in global configuration mode. To return to the default setting, use the **no** form of this command.

ipv6 neighbor binding stale-lifetime {*value* | **infinite**}

no ipv6 neighbor binding

Syntax Description

value	The maximum time, in minutes, a stale entry is kept in the table before it is deleted or some proof of reachability is seen. The range is from 1 to 3600 minutes, and the default is 24 hours (or 1440 minutes).
infinite	Keeps an entry in the binding table for an infinite amount of time.

Command Default

Stale lifetime: 1440 minutes (24 hours)

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

Use the **ipv6 neighbor binding stale-lifetime** command to configure the length of time a stale entry is kept in the binding table before it is removed.

Examples

The following example shows how to change the stale lifetime for a binding entry to 720 minutes (or 12 hours):

```
Router(config)# ipv6 neighbor binding stale lifetime 720
```

Related Commands

Command	Description
ipv6 neighbor binding	Changes the defaults of neighbor binding entries in a binding table.

ipv6 neighbor binding vlan

To add a static entry to the binding table database, use the **ipv6 neighbor binding vlan** command in global configuration mode. To remove the static entry, use the **no** form of this command.

ipv6 neighbor binding vlan *vlan-id* {**interface** *type number* | *ipv6-address* | *mac-address*} [**tracking** [**disable** | **enable** | **retry-interval** *value*] | **reachable-lifetime** *value*]

no ipv6 neighbor binding vlan *vlan-id*

Syntax Description

vlan-id	ID of the specified VLAN.
interface *type number*	Static entries by the specified interface type and number.
ipv6-address	Static entries by the specified IPv6 address.
mac-address	Static entries by the specified Media Access Control (MAC) address.
tracking	(Optional) Verifies a static entry's reachability directly.
disable	(Optional) Disables tracking for a particular static entry.
enable	(Optional) Enables tracking for a particular static entry.
retry-interval *value*	(Optional) Verifies a static entry's reachability, in seconds, at the configured interval. The range is from 1 to 3600 seconds, and the default is 300 seconds.
reachable-lifetime *value*	(Optional) The maximum time, in seconds, an entry is considered reachable without getting a proof of reachability (direct reachability through tracking, or indirect reachability through Neighbor Discovery protocol [NDP] inspection). After that, the entry is moved to stale. The range is from 1 to 3600 seconds, and the default is 300 seconds.

Command Default

Retry interval: 300 seconds
Reachable lifetime: 300 seconds

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

The **ipv6 neighbor binding vlan** command is used to control the content of the binding table. Use this command to add a static entry in the binding table database. The binding table manager is responsible for aging out entries and verifying their reachability directly by probing them (if the **tracking** keyword is enabled). Use of the **tracking** keyword overrides any general behavior provided globally by the **ipv6 neighbor tracking** command for this static entry. The **disable** keyword disables for tracking for this static entry. The **stale-lifetime** keyword defines the maximum time the entry will be kept once it is determined to be not reachable (or "stale").

Examples

The following example shows how to change the reachable lifetime for binding entries to 100 seconds:

```
Router(config)# ipv6 neighbor binding reachable-entries 100
```

Related Commands

Command	Description
ipv6 neighbor binding max-entries	Specifies the maximum number of entries that are allowed to be inserted in the cache.
ipv6 neighbor tracking	Tracks entries in the binding table.

ipv6 neighbor tracking

To track entries in the binding table, use the **ipv6 neighbor tracking** command in global configuration mode. To disable entry tracking, use the **no** form of the command.

ipv6 neighbor tracking [**retry-interval** *value*]

no ipv6 neighbor tracking [**retry-interval** *value*]

Syntax Description

retry-interval *value*	(Optional) Verifies a static entry's reachability at the configured interval time between two probings. The *value* argument is in seconds, the range is from 1 to 3600 seconds, and the default is 300 seconds.

Command Default

Retry interval: 300 seconds
Reachable lifetime: 300 seconds
Stale lifetime: 1440 minutes
Down lifetime: 1440 minutes

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

The **ipv6 neighbor tracking** command enables the tracking of entries in the binding table. Entry reachability is tested at every interval configured by the optional **retry-interval** keyword (or every 300 seconds, which is the default retry interval) using the neighbor unreachability detection (NUD) mechanism used for directly tracking neighbor reachability.

Reachability can also be established indirectly by using Neighbor Discovery Protocol [NDP] inspection up to the VERIFY_MAX_RETRIES value (the default is 10 seconds). When there is no response, entries are considered stale and are deleted after the stale lifetime value is reached (the default is 1440 minutes).

When the **ipv6 neighbor tracking** command is not enabled, entries are considered stale after the reachable lifetime value is met (the default is 300 seconds), and deleted after the stale lifetime value is met.

To change the default values of neighbor binding entries in a binding table, use the **ipv6 neighbor binding** command.

Examples

The following example shows how to track entries in a binding table:

```
Router(config)# ipv6 neighbor tracking
```

Related Commands

Command	Description
ipv6 neighbor binding	Changes the defaults of neighbor binding entries in a binding table.

ipv6 next-hop-self eigrp

To instruct the router configured with Enhanced Interior Gateway Routing Protocol (EIGRP) that the IPv6 next hop is itself, use the **ipv6 next-hop-self eigrp** command in interface configuration mode. To instruct EIGRP to use the received next hop rather than itself, use the **no** form of this command.

ipv6 next-hop-self eigrp *as-number*

no ipv6 next-hop-self eigrp *as-number*

Syntax Description

as-number	Autonomous system number.

Command Default

EIGRP always sets the IPv6 next-hop value to be itself.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(6)T	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.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

EIGRP will, by default, set the IPv6 next-hop value to be itself for routes that it is advertising, even when advertising those routes back out the same interface where it learned them. To change this default, use the **no ipv6 next-hop-self eigrp** command to instruct EIGRP to use the received next-hop value when advertising these routes. Some exceptions to this guideline are as follows:

- If spoke-to-spoke dynamic tunnels are not wanted, then the **no ipv6 next-hop-self eigrp** command is not needed.
- If spoke-to-spoke dynamic tunnels are wanted, then you must use process switching on the tunnel interface on the spoke routers.

Examples

The following example changes the default IPv6 next-hop value and instructs EIGRP to use the received next-hop value:

```
interface serial 0
 no ipv6 next-hop-self eigrp 1
```

ipv6 nhrp authentication

To configure the authentication string for an interface using the Next Hop Resolution Protocol (NHRP), use the **ip nhrp authentication** command in interface configuration mode. To remove the authentication string, use the **no** form of this command.

ipv6 nhrp authentication *string*

no ipv6 nhrp authentication [*string*]

Syntax Description

string	Authentication string configured for the source and destination stations that controls whether NHRP stations allow intercommunication. The string can be up to eight characters long.

Command Default

No authentication string is configured. Cisco IOS software adds no authentication option to NHRP packets it generates.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

All routers configured with NHRP within one logical nonbroadcast multiaccess (NBMA) network must share the same authentication string.

Examples

In the following example, the authentication string named examplexx must be configured in all devices using NHRP on the interface before NHRP communication occurs:

```
ip nhrp authentication examplexx
```

ipv6 nhrp holdtime

To change the number of seconds that Next Hop Resolution Protocol (NHRP) nonbroadcast multiaccess (NBMA) addresses are advertised as valid in authoritative NHRP responses, use the **ipv6 nhrp holdtime** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ipv6 nhrp holdtime *seconds*

no ipv6 nhrp holdtime [*seconds*]

Syntax Description

seconds	Time, in seconds, that NBMA addresses are advertised as valid in positive authoritative NHRP responses.

Command Default

7200 seconds (2 hours)

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

The **ipv6 nhrp holdtime** command affects authoritative responses only. The advertised holding time is the length of time the Cisco IOS software tells other routers to keep information that it is providing in authoritative NHRP responses. The cached IPv6-to-NBMA address mapping entries are discarded after the holding time expires.

The NHRP cache can contain static and dynamic entries. The static entries never expire. Dynamic entries expire regardless of whether they are authoritative or nonauthoritative.

Examples

In the following example, NHRP NBMA addresses are advertised as valid in positive authoritative NHRP responses for 1 hour:

```
ipv6 nhrp holdtime 3600
```

ipv6 nhrp interest

To control which IPv6 packets can trigger sending a Next Hop Resolution Protocol (NHRP) request packet, use the **ipv6 nhrp interest** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ipv6 nhrp interest *ipv6-access-list*

no ipv6 nhrp interest [*ipv6-access-list*]

Syntax Description

ipv6-access-list	IPv6 access list number in the range from 1 to 199.

Command Default

All non-NHRP packets can trigger NHRP requests.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

Use the **ipv6 nhrp interest** command with the **ipv6 access-list** command to control which IPv6 packets trigger NHRP requests.

Examples

In the following example, the IPv6 packets specified by the IPv6 access list named list2 will trigger NHRP requests:

```
Router(config)# ipv6 access-list list2 permit any any
Router(config-if)# ipv6 nhrp interest list2
```

Related Commands

Command	Description
ipv6 access-list	Defines an IPv6 access list.

ipv6 nhrp map

To statically configure the IPv6-to-nonbroadcast multiaccess (NBMA) address mapping of IPv6 destinations connected to an NBMA network, use the **ipv6 nhrp map** command in interface configuration mode. To remove the static entry from Next Hop Resolution Protocol (NHRP) cache, use the **no** form of this command.

ipv6 nhrp map *ipv6-address nbma-address*

no ipv6 nhrp map *ipv6-address nbma-address*

Syntax Description

ipv6-address	IPv6 address of the destinations reachable through the NBMA network. This address is mapped to the NBMA address.
nbma-address	NBMA address that is directly reachable through the NBMA network. The address format varies depending on the medium you are using. For example, ATM has a network service access point (NSAP) address, Ethernet has a MAC address, and Switched Multimegabit Data Service (SMDS) has an E.164 address. This address is mapped to the IPv4 address.

Command Default

No static IPv6-to-NBMA cache entries exist.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

The **ipv6 nhrp map** command accepts IPv6 prefixes in the form of **prefix/***prefix-length*, as shown in the following example:

```
ipv6 nhrp map abcd::abcd/128 172.16.1.1
```

Because the NBMA is IPv4, only IPv4 destinations are accepted in the **ipv6 nhrp map** command. IPv6 prefixes can be mapped to IPv4 addresses.

You will probably need to configure at least one static mapping in order to reach the next hop server. Repeat this command to statically configure multiple IPv6-to-NBMA address mappings.

Examples

In the following example, this station in a multipoint tunnel network is statically configured to be served by two next hop servers 2001:0DB8:3333:4::5 and 2001:0DB8:4444:5::6. The NBMA address for 2001:0DB8:3333:4::5 is statically configured to be 2001:0DB8:5555:5::6 and the NBMA address for 2001:0DB8:4444:5::6 is 2001:0DB8:8888:7::6.

```
interface tunnel 0
 ipv6 nhrp nhs 2001:0DB8:3333:4::5
```

```
ipv6 nhrp nhs 2001:0DB8:4444:5::6
ipv6 nhrp map 2001:0DB8:3333:4::5 10.1.1.1
ipv6 nhrp map 2001:0DB8:4444:5::6 10.2.2.2
```

ipv6 nhrp map multicast

To map destination IPv6 addresses to IPv4 nonbroadcast multiaccess (NBMA) addresses, use the **ipv6 nhrp map multicast** command in interface configuration mode. To remove the destinations, use the **no** form of this command.

ipv6 nhrp map multicast *ipv4-nbma-address*

no ipv6 nhrp map multicast *ipv4-nbma-address*

Syntax Description

ipv4-nbma-address	IPv4 NBMA address (IPv6 over IPv4 transport) that is directly reachable through the NBMA network.

Command Default

No NBMA addresses are configured as destinations for broadcast or multicast packets.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

The **ipv6 nhrp map multicast** command works only with tunnel interfaces.

The command is useful for supporting broadcasts over a tunnel network when the underlying network does not support IPv4 multicast. If the underlying network does support IPv4 multicast, you should use the **tunnel destination** command to configure a multicast destination for transmission of tunnel broadcasts or multicasts.

When multiple NBMA addresses are configured, the system replicates the broadcast packet for each address.

Examples

In the following example, the IPv6 address is mapped to the IPv4 address 10.11.11.99:

```
ipv6 nhrp map 2001:0DB8::99/128 10.11.11.99
 ipv6 nhrp map multicast 10.11.11.99
```

Related Commands

Command	Description
tunnel destination	Specifies the destination for a tunnel interface.

ipv6 nhrp map multicast dynamic

To allow Next Hop Resolution Protocol (NHRP) to automatically add routers to the multicast NHRP mappings, use the **ipv6 nhrp map multicast dynamic** command in interface configuration mode. To disable this functionality, use the **no** form of this command

ipv6 nhrp map multicast dynamic

no ipv6 nhrp map multicast dynamic

Syntax Description

This command has no arguments or keywords.

Command Default

Routers are not automatically added to the multicast NHRP mapping.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

Use the **ipv6 nhrp map multicast dynamic** command when spoke routers need to initiate multipoint generic routing encapsulation (GRE) and IP security (IPsec) tunnels and register their unicast NHRP mappings. This command is needed to enable dynamic routing protocols to work over the Multipoint GRE and IPsec tunnels because IGP routing protocols use multicast packets. This command prevents the hub router from needing a separate configuration line for a multicast mapping for each spoke router.

Examples

The following example shows how to enable the **ipv6 nhrp map multicast dynamic** command on the hub router:

```
crypto ipsec profile cisco-ipsec
 set transform-set cisco-ts
!
interface Tunnel0
 bandwidth 100000
 ip address 10.1.1.99 255.255.255.0
 no ip redirects
 ip nhrp map multicast dynamic
 delay 50000
 ipv6 address 2001:0DB8::99/100
 ipv6 address FE80::0B:0B:0B:8F link-local
 ipv6 enable
 ipv6 eigrp 1
 no ipv6 split-horizon eigrp 1
 no ipv6 next-hop-self eigrp 1
 ipv6 nhrp map multicast dynamic
 ipv6 nhrp network-id 99
 tunnel source Ethernet0/0
 tunnel mode gre multipoint
```

```
tunnel protection ipsec profile cisco-ipsec
```

Related Commands

Command	Description
ipv6 nhrp network-id	Enables NHRP on an interface.

ipv6 nhrp max-send

To change the maximum frequency at which Next Hop Resolution Protocol (NHRP) packets can be sent, use the **ipv6 nhrp max-send** command in interface configuration mode. To restore this frequency to the default value, use the **no** form of this command.

ipv6 nhrp max-send *pkt-count* **every** *seconds*

no ipv6 nhrp max-send

Syntax Description

pkt-count	Number of packets that can be sent in the range from 1 to 65535. Default is 100 packets.
every *seconds*	Specifies the time (in seconds) in the range from 10 to 65535. Default is 10 seconds.

Command Default

Maximum frequency default settings are used.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

The software maintains a per-interface quota of NHRP packets that can be sent. NHRP traffic, whether locally generated or forwarded, cannot be sent at a rate that exceeds this quota. The quota is replenished at the rate specified by the *seconds* argument:

- The user needs to consider the number of spoke routers being handled by this hub and how often they send NHRP registration requests. To support this load you would need:

  Number of spokes / registration timeout * *max-send-interval*

  - Example:

    500 spokes with 100-second registration timeout

    Max send value = 500/100*10 = 50

- The maximum number of spoke-spoke tunnels that are expected to be up at any one time across the whole DMVPN network.

  spoke-spoke tunnels/NHRP holdtime * max-send-interval

  This formula covers spoke-spoke tunnel creation and the refreshing of spoke-spoke tunnels that are used for longer periods of time:

  - Example

    2000 spoke-spoke tunnels with 250-second hold timeout

    Max send value = 2000/250*10 = 80

Then add these together and multiply this by 1.5 to give a buffer:

  - Example

    Max send = (50 + 80) * 2 = 260

- The max-send interval can be used to keep the long-term average number of NHRP messages allowed to be sent constant, but to allow greater peaks:

  - Example

    400 messages in 10 seconds

  In this case, it could peak at approximately 200 messages in the first second of the 10-second interval, but still keep to a 40-messages-per-second average over the 10-second interval:

    4000 messages in 100 seconds

  In this case, it could peak at approximately 2000 messages in the first second of the 100-second interval, but it would still be held to 40-messages-per-second average over the 100-second interval. In the second case, it could handle a higher peak rate, but risk a longer period of time when no messages can be sent if it used up its quota for the interval.

By default, the maximum rate at which the software sends NHRP packets is five packets per 10 seconds. The software maintains a per-interface quota of NHRP packets (whether generated locally or forwarded) that can be sent.

Examples

In the following example, only one NHRP packet can be sent from serial interface 0 each minute:

```
interface serial 0
 ipv6 nhrp max-send 1 every 60
```

Related Commands

Command	Description
ipv6 nhrp interest	Controls which IP packets can trigger sending an NHRP request.
ipv6 nhrp use	Configures the software so that NHRP is deferred until the system has attempted to send data traffic to a particular destination multiple times.

ipv6 nhrp network-id

To enable the Next Hop Resolution Protocol (NHRP) on an interface, use the **ipv6 nhrp network-id** command in interface configuration mode. To disable NHRP on the interface, use the **no** form of this command.

ipv6 nhrp network-id *network-id*

no ipv6 nhrp network-id *network-id*

Syntax Description

network-id	Globally unique, 32-bit network identifier from a nonbroadcast multiaccess (NBMA) network. The range is from 1 to 4294967295.

Command Default

NHRP is disabled on the interface.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

In general, all NHRP stations within one logical NBMA network must be configured with the same network identifier.

Examples

The following example shows how to enable NHRP on the interface:

```
Router(config-if)# ipv6 nhrp network-id 99
```

Related Commands

Command	Description
ipv6 nhrp map multicast dynamic	Allows NHRP to automatically add routers to the multicast NHRP mappings.

ipv6 nhrp nhs

To specify the IPv6 prefix of one or more Next Hop Resolution Protocol (NHRP) servers, use the **ipv6 nhrp nhs** command in interface configuration mode. To remove the address, use the **no** form of this command.

ipv6 nhrp nhs {*ipv6-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 ipv6 nhrp nhs {*ipv6-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

ipv6-nhs-address	IPv6 prefix of the next hop server being specified.
nbma	(Optional) Specifies nonbroadcast multiple access (NBMA) values.
nbma-address	IPv6 NBMA address.
FQDN-string	Next hop address (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 need 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.

Command Default

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
12.4(20)T	This command was introduced.
15.1(2)T	This command was modified. The *net-address* argument was 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 **ipv6 nhrp nhs** command to specify the IPv6 prefix 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 IPv6 prefixes 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 IPv6 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)# ipv6 nhrp nhs 2001:0DB8:3333:4::5 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)# ipv6 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)# ipv6 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)# ipv6 nhrp nhs 2001:0DB8:3333:4::5 priority 1 cluster 2
```

Related Commands

Command	Description
ipv6 nhrp map	Statically configures the IP-to-NBMA address mapping of IPv6 destinations connected to an NBMA network.
show ipv6 nhrp	Displays NHRP mapping information.

ipv6 nhrp record

To reenable the use of forward record and reverse record options in Next Hop Resolution Protocol (NHRP) request and reply packets, use the **ipv6 nhrp record** command in interface configuration mode. To suppress the use of such options, use the **no** form of this command.

ipv6 nhrp record

no ipv6 nhrp record

Syntax Description

This command has no arguments or keywords.

Command Default

Forward record and reverse record options are used in NHRP request and reply packets.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

Forward record and reverse record options provide loop detection and are enabled by default. Using the **no** form of this command disables this method of loop detection. For another method of loop detection, see the **ipv6 nhrp responder** command.

Examples

The following example suppresses forward record and reverse record options:

```
no ipv6 nhrp record
```

Related Commands

Command	Description
ipv6 nhrp responder	Designates the primary IP address of which interface the next hop server will use in NHRP reply packets when the NHRP requester uses the Responder Address option.

ipv6 nhrp redirect

To enable Next Hop Resolution Protocol (NHRP) redirect, use the **ipv6 nhrp redirect** command in interface configuration mode. To remove the NHRP redirect, use the **no** form of this command.

ipv6 nhrp redirect [**timeout** *seconds*]

no ipv6 nhrp redirect [**timeout** *seconds*]

Syntax Description

timeout *seconds*	(Optional) Indicates the interval, in seconds, that the NHRP redirects are sent for the same nonbroadcast multiaccess (NBMA) source and destination combination. The range is from 2 to 30 seconds.

Command Default

NHRP redirect is disabled.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

The NHRP redirect message is an indication that the current path to the destination is not optimal. The receiver of the message should find a better path to the destination.

This command generates an NHRP redirect traffic indication message if the incoming and outgoing interface is part of the same dynamic multipoint VPN (DMVPN) network. The NHRP shortcut switching feature depends on receiving the NHRP redirect message. NHRP shortcut switching does not trigger an NHRP resolution request on its own. It triggers an NHRP resolution request only after receiving an NHRP redirect message.

Most of the traffic would follow a spoke-hub-spoke path. NHRP redirect is generally required to be configured on all the DMVPN nodes in the event the traffic follows a spoke-spoke-hub-spoke path.

Do not configure this command if the DMVPN network is configured for full-mesh. In a full-mesh configuration, the spokes are populated with a full routing table, with the next hop being the other spokes.

Examples

The following example shows how to enable NHRP redirects on the interface:

```
ipv6 nhrp redirect
```

Related Commands

Command	Description
ipv6 nhrp shortcut	Enables NHRP shortcut switching.

ipv6 nhrp registration

To enable the client to set the unique flag in the Next Hop Resolution Protocol (NHRP) request and reply packets, use the **ipv6 nhrp registration** command in interface configuration mode. To reenable this functionality, use the **no** form of this command.

ipv6 nhrp registration [**timeout** *seconds* | **no-unique**]

no ipv6 nhrp registration [**timeout** *seconds* | **no-unique**]

Syntax Description

timeout *seconds*	(Optional) Specifies the time between periodic registration messages: • *seconds*—Number of seconds. The range is from 1 through the value of the NHRP hold timer. • If the **timeout** keyword is not specified, NHRP registration messages are sent every number of seconds equal to one-third the value of the NHRP hold timer.
no-unique	(Optional) Enables the client to not set the unique flag in the NHRP request and reply packets.

Command Default

The default settings are used.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

If the unique flag is set in the NHRP registration request packet, a next hop server (NHS) must reject any registration attempts for the same private address using a different nonbroadcast multiaccess (NBMA) address. If a client receives a new IP address–for example, via DHCP–and tries to register before the cache entry on the NHS times out, the NHS must reject it.

By configuring the **ip nhrp registration** command and **no-unique** keyword, the unique flag is not set, and the NHS can override the old registration information.

This command and keyword combination is useful in an environment where client IPv6 addresses can change frequently such as a dial environment.

Examples

The following example configures the client not to set the unique flag in the NHRP registration packet:

```
interface FastEthernet 0/0
 ipv6 nhrp registration no-unique
```

The following example shows that the registration timeout is set to 120 seconds, and the delay is set to 5 seconds:

```
interface FastEthernet 0/0
 ipv6 nhrp registration 120 5
```

Related Commands

Command	Description
ipv6 nhrp holdtime	Changes the number of seconds that NHRP NBMA addresses are advertised as valid in authoritative NHRP responses

ipv6 nhrp responder

To designate the primary IPv6 address the next hop server that an interface will use in Next Hop Resolution Protocol (NHRP) reply packets when the NHRP requestor uses the Responder Address option, use the **ipv6 nhrp responder** command in interface configuration mode. To remove the designation, use the **no** form of this command.

ipv6 nhrp responder *interface-type interface-number*

no ipv6 nhrp responder [*interface-type*] [*interface-number*]

Syntax Description

interface-type	Interface type whose primary IPv6 address is used when a next hop server complies with a Responder Address option (for example, **serial** or **tunnel**).
interface-number	Interface number whose primary IPv6 address is used when a next hop server complies with a Responder Address option.

Command Default

The next hop server uses the IPv6 address of the interface where the NHRP request was received.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

If an NHRP requestor wants to know which next hop server generates an NHRP reply packet, it can request that information through the Responder Address option. The next hop server that generates the NHRP reply packet then complies by inserting its own IPv6 address in the Responder Address option of the NHRP reply. The next hop server uses the primary IPv6 address of the specified interface.

If an NHRP reply packet being forwarded by a next hop server contains the IPv6 address of that next hop server, the next hop server generates an Error Indication of type “NHRP Loop Detected” and discards the reply packet.

Examples

In the following example, any NHRP requests for the Responder Address will cause this router acting as a next hop server to supply the primary IPv6 address of serial interface 0 in the NHRP reply packet:

```
ipv6 nhrp responder serial 0
```

ipv6 nhrp server-only

To configure the interface to operate in Next Hop Resolution Protocol (NHRP) server-only mode, use the **ipv6 nhrp server-only** command in interface configuration mode. To disable this feature, use the **no** form of this command.

ipv6 nhrp server-only [**non-caching**]

no ipv6 nhrp server-only

Syntax Description

non-caching	(Optional) Specifies that the router will not cache NHRP information received on this interface.

Command Default

The interface does not operate in NHRP server-only mode.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

When the interface is operating in NHRP server-only mode, the interface does not originate NHRP requests or set up an NHRP shortcut Switched Virtual Circuit (SVC).

Examples

The following example shows that the interface is configured to operate in server-only mode:

```
ipv6 nhrp server-only
```

ipv6 nhrp shortcut

To enable Next Hop Resolution Protocol (NHRP) shortcut switching, use the **ipv6 nhrp shortcut** command in interface configuration mode. To remove shortcut switching from NHRP, use the **no** form of this command.

ipv6 nhrp shortcut

no ipv6 nhrp shortcut

Syntax Description

This command has no arguments or keywords.

Command Default

NHRP shortcut switching is disabled.

Command Modes

Interface configuration (config-if)#

Command History

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

Usage Guidelines

Do not configure this command if the dynamic multipoint VPN (DMVPN) network is configured for full-mesh. In a full-mesh configuration, the spokes are populated with a full routing table, with the next hop being the other spokes.

Examples

The following example shows how to configure an NHRP shortcut on an interface:

```
Router(config-if)# ipv6 nhrp shortcut
```

Related Commands

Command	Description
ipv6 nhrp redirect	Enables NHRP redirect.

ipv6 nhrp trigger-svc

To configure when the Next Hop Resolution Protocol (NHRP) will set up and tear down a switched virtual circuit (SVC) based on aggregate traffic rates, use the **ipv6 nhrp trigger-svc** command in interface configuration mode. To restore the default thresholds, use the **no** form of this command.

ipv6 nhrp trigger-svc *trigger-threshold teardown-threshold*

no ipv6 nhrp trigger-svc

Syntax Description

trigger-threshold	Average traffic rate calculated during the load interval, at or above which NHRP will set up an SVC for a destination. The default value is 1 kb/s.
teardown-threshold	Average traffic rate calculated during the load interval, at or below which NHRP will tear down the SVC to the destination. The default value is 0 kb/s.

Command Default

The SVC default settings are used.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

The two thresholds are measured during a sampling interval of 30 seconds, by default.

Examples

In the following example, the triggering and teardown thresholds are set to 100 kb/s and 5 kb/s, respectively:

```
ipv6 nhrp trigger-svc 100 5
```

ipv6 nhrp use

To configure the software so that the Next Hop Resolution Protocol (NHRP) is deferred until the system has attempted to send data traffic to a particular destination multiple times, use the **ipv6 nhrp use** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ipv6 nhrp use *usage-count*

no ipv6 nhrp use *usage-count*

Syntax Description

usage-count	Packet count in the range from 1 to 65535. Default is 1.

Command Default

The first time a data packet is sent to a destination for which the system determines NHRP can be used, an NHRP request is sent.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

When the software attempts to send a data packet to a destination for which it has determined that NHRP address resolution can be used, an NHRP request for that destination normally is sent immediately. Configuring the *usage-count* argument causes the system to wait until the configured number of data packets have been sent to a particular destination before it attempts NHRP. The *usage-count* argument for a particular destination is measured over 1-minute intervals (the NHRP cache expiration interval).

The usage count applies *per destination*. So if the *usage-count* argument is configured to be 3, and four data packets are sent toward 2001:0DB8:3333:4::5 and one packet toward 2001:0DB8:5555:5::6, then an NHRP request is generated for 2001:0DB8:3333:4::5 only.

If the system continues to need to forward data packets to a particular destination, but no NHRP response has been received, retransmission of NHRP requests is performed. This retransmission occurs only if data traffic continues to be sent to a destination.

The **ipv6 nhrp interest** command controls *which* packets cause NHRP address resolution to take place; the **ipv6 nhrp use** command controls *how readily* the system attempts such address resolution.

Examples

In the following example, if in the first minute five packets are sent to the first destination and five packets are sent to a second destination, then a single NHRP request is generated for the second destination.

If in the second minute the same traffic is generated and no NHRP responses have been received, then the system resends its request for the second destination.

```
ipv6 nhrp use 5
```

Related Commands

Command	Description
ipv6 nhrp interest	Controls which IPv6 packets can trigger sending an NHRP request.
ipv6 nhrp max-send	Changes the maximum frequency at which NHRP packets can be sent.

ipv6 ospf area

To enable Open Shortest Path First version 3 (OSPFv3) on an interface, use the **ipv6 ospf area** command in interface configuration mode. To disable OSPFv3 routing for interfaces defined, use the **no** form of this command.

ipv6 ospf *process-id* **area** *area-id* [**instance** *instance-id*]

no ipv6 ospf *process-id* **area** *area-id* [**instance** *instance-id*]

Syntax Description

process-id	Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when enabling the OSPFv3 routing process.
area-id	Area that is to be associated with the OSPFv3 interface.
instance *instance-id*	(Optional) Instance identifier.

Command Default

OSPFv3 is not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
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.
12.2(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.
15.1(3)S	Use of the **ospfv3 area** command can affect the **ipv6 ospf area** command.
Cisco IOS XE Release 3.4S	Use of the **ospfv3 area** command can affect the **ipv6 ospf area** command.
15.2(1)T	Use of the **ospfv3 area** command can affect the **ipv6 ospf area** command.

Usage Guidelines

If the **ospfv3 area** command is configured with the *process-id* argument, it overwrites the **ipv6 ospf area** configuration if OSPFv3 was attached to the interface using the **ipv6 ospf area** command.

Before you enable OSPFv3 on an interface using the **ipv6 ospf area** command, you must enable IPv6 on the interface, and you must enable IPv6 routing.

An OSPFv3 instance (also known as an OSPFv3 process) can be considered a logical router running OSPFv3 in a physical router. Use the instance ID to control selection of other routers as your neighbors. You become neighbors only with routers that have the same instance ID.

In IPv6, users can configure many addresses on an interface. In OSPFv3, all addresses on an interface are included by default. Users cannot select some addresses to be imported into OSPFv3; either all addresses on an interface are imported, or no addresses on an interface are imported.

There is no limit to the number of **ipv6 ospf area** commands you can use on the router. You must have at least two interfaces configured for OSPFv3 to run.

Examples

The following example enables OSPFv3 on an interface:

```
ipv6 unicast-routing
interface ethernet0/1
  ipv6 enable
  ipv6 ospf 1 area 0

ipv6 unicast-routing
interface ethernet0/2
  ipv6 enable
  ipv6 ospf 120 area 1.4.20.9 instance 2
```

Related Commands

Command	Description
ipv6 router ospf	Enables OSPFv3 router configuration mode.
ospfv3 area	Enables an OSPFv3 instance with the IPv4 or IPv6 address family.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

ipv6 ospf authentication

To specify the authentication type for an Open Shortest Path First (OSPFv3) version 3 interface, use the **ipv6 ospf authentication** command in interface configuration mode. To remove the authentication type for an interface, use the **no** form of this command.

ipv6 ospf authentication ipsec spi *spi* {**md5** | **sha1**} [*key-encryption-type* {*key* | **null**}]

no ipv6 ospf authentication ipsec spi *spi*

Syntax Description

ipsec	IP Security (IPsec).
spi *spi*	Security policy index (SPI) value. The *spi* value must be a number from 256 to 4294967295, which is entered as a decimal.
md5	Enables message digest 5 (MD5) authentication.
sha1	Enables Secure Hash Algorithm 1 (SHA-1) authentication.
key-encryption-type	(Optional) One of two values can be entered: • **0**—The key is not encrypted. • **7**—The key is encrypted.
key	Number used in the calculation of the message digest. When MD5 authentication is used, the key must be 32 hex digits (16 bytes) long. When SHA-1 authentication is used, the key must be 40 hex digits (20 bytes) long.
null	Used to override area authentication.

Command Default

No authentication.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.4(4)T	The **sha1** keyword was added.
15.1(3)S	Use of the **ospfv3 authentication** command can affect the **ipv6 ospf authentication** command.
Cisco IOS XE Release 3.4S	Use of the **ospfv3 authentication** command can affect the **ipv6 ospf authentication** command.
15.2(1)T	Use of the **ospfv3 authentication** command can affect the **ipv6 ospf authentication** command.

Usage Guidelines

The user needs to ensure that the same policy (the SPI and the key) is configured on all of the interfaces on the link. SPI values may automatically be used by other client applications, such as tunnels.

The policy database is common to all client applications on a box. This means that two IPsec clients, such as OSPF v3 and a tunnel, cannot use the same SPI. Additionally, an SPI can be used only in one policy.

The **null** keyword is used to override existing area authentication. If area authentication is not configured, then it is not necessary to configure the interface with the **ipv6 ospf authentication null** command.

Beginning with Cisco IOS Release 12.4(4)T, the **sha1** keyword can be used to choose SHA-1 authentication instead of entering the **md5** keyword to use MD5 authentication. The SHA-1 algorithm is considered to be somewhat more secure than the MD5 algorithm, and requires a 40 hex digit (20-byte) key rather than the 32 hex digit (16-byte) key that is required for MD5 authentication.

Examples

The following example enables MD5 authentication and then overrides area authentication:

```
Router(config-if)# ipv6 ospf authentication ipsec spi 500 md5
1234567890abcdef1234567890abcdef
Router(config-if)# ipv6 ospf authentication null
```

The following example enables SHA-1 authentication on the interface:

```
Router(config)# interface Ethernet0/0
Router(config)# ipv6 enable
Router(config-if)# ipv6 ospf authentication ipsec spi 500 sha1
1234567890123456789012345678901234567890
```

Related Commands

Command	Description
ipv6 router ospf	Enables OSPF router configuration mode.
ospfv3 authentication	Specifies the authentication type for an OSPFv3 instance.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

ipv6 ospf bfd

To enable Bidirectional Forwarding Detection (BFD) on a specific interface configured for Open Shortest Path First version 3 (OSPFv3), use the **ipv6 ospf bfd** command in interface configuration mode.To remove the **ospf bfd** command, use the **no** form of this command.

ipv6 ospf bfd [**disable**]

no ipv6 ospf bfd

Syntax Description

disable	(Optional) Disables BFD for OSPFv3 on a specified interface.

Command Default

When the **disable** keyword is not used, the default behavior is to enable BFD support for OSPFv3 on the interface.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
15.1(3)S	Use of the **ospfv3 bfd** command can affect the **ipv6 ospf bfd** command.
Cisco IOS XE Release 3.4S	Use of the **ospfv3 bfd** command can affect the **ipv6 ospf bfd** command.
15.2(1)T	Use of the **ospfv3 bfd** command can affect the **ipv6 ospf bfd** command.

Usage Guidelines

Enter the **ipv6 ospf bfd** command to configure an OSPFv3 interface to use BFD for failure detection. If you have used the **bfd all-interfaces** command in router configuration mode to globally configure all OSPFv3 interfaces for an OSPFv3 process to use BFD, you can enter the **ipv6 ospf bfd** command in interface configuration mode with the **disable** keyword to disable BFD for a specific OSPFv3 interface.

Examples

In the following example, the interface associated with OSPFv3, Fast Ethernet interface 3/0, is configured for BFD:

```
Router> enable
Router# configure terminal
Router(config)# interface fastethernet 3/0
Router(config-if)# ipv6 ospf bfd
Router(config-if)# end
```

Related Commands

Command	Description
bfd all-interfaces	Enables BFD for all interfaces for a BFD peer.
ospfv3 bfd	Enables BFD on an interface.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

ipv6 ospf cost

To explicitly specify the cost of sending a packet on an Open Shortest Path First version 3 (OSPFv3) interface, use the **ipv6 ospf cost** command in interface configuration mode. To reset the interface cost to the default value, use the **no** form of this command.

ipv6 ospf cost *interface-cost* | *dynamic* [**weight** {**throughput** *percent* | **resources** *percent* | **latency** *percent* | **L2-factor** *percent*] | [**hysteresis** [**threshold** *threshold-value*]]

no ipv6 ospf cost

Syntax Description

interface-cost	Unsigned integer value expressed as the link-state metric. It can be a value in the range from 1 to 65535.
dynamic	Default value on VMI interfaces.
weight	(Optional) Amount of impact a variable has on the dynamic cost.
throughput *percent*	Throughput weight of the Layer 2 link, expressed as a percentage. The *percent* value can be in the range from 0 to 100. The default value is 100.
resources *percent*	Resources weight (such as battery life) of the router at the Layer 2 link, expressed as a percentage. The *percent* value can be in the range from 0 to 100. The default value is 100.
latency *percent*	Latency weight of the Layer 2 link, expressed as a percentage. The *percent* value can be in the range from 0 to 100. The default value is 100.
L2-factor *percent*	Quality weight of the Layer 2 link expressed as a percentage. The *percent* value can be in the range from 0 to 100. The default value is 100.
hysteresis	(Optional) Value used to dampen cost changes.
threshold *threshold-value*	(Optional) Cost change threshold at which hysteresis will be implemented. The threshold range is from 0 to 64k, and the default threshold value is 10k.

Command Default

Default cost is based on the bandwidth.
Default cost on VMI interfaces is dynamic.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)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.

Release	Modification
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(15)XF	The following keywords and arguments were added to support Virtual Multipoint Interfaces (VMI) and Mobile Adhoc Networking: • *dynamic* argument • **weight**, **throughput** *percent*, **resources** *percent*, **latency** *percent*, and **L2-factor** *percent* keywords and arguments • **hysteresis** and **threshold** keywords and the *threshold-value* argument
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
15.1(3)S	Use of the **ospfv3 cost** command can affect the **ipv6 ospf cost** command.
Cisco IOS XE Release 3.4S	Use of the **ospfv3 cost** command can affect the **ipv6 ospf cost** command.
15.2(1)T	Use of the **ospfv3 cost** command can affect the **ipv6 ospf cost** command.

Usage Guidelines

When the **ospfv3 cost** command is configured with the *process-id* argument, it overwrites the **ipv6 ospf cost** configuration if OSPFv3 was attached to the interface using the **ipv6 ospf area** command.

Changing the Default Cost

You can set the metric manually using the **ipv6 ospf cost** command, if you need to change the default.

Using the **bandwidth** command changes the link cost as long as the **ipv6 ospf cost** command is not used.

The link-state metric is advertised as the link cost in the router link advertisement.

Dynamic Cost Metric for Interfaces

The dynamic cost metric used for interfaces is computed based on the Layer 2 (L2) feedback to Layer 3 (L3).

In general, the path cost is calculated using the following formula:

Using this formula, the default path costs were calculated as noted in the following list. If these values do not suit your network, you can use your own method of calculating path costs.

- 56-kbps serial link—Default cost is 1785.
- 64-kbps serial link—Default cost is 1562.
- T1 (1.544-Mbps serial link)—Default cost is 64.
- E1 (2.048-Mbps serial link)—Default cost is 48.
- 4-Mbps Token Ring—Default cost is 25.
- Ethernet—Default cost is 10.
- 16-Mbps Token Ring—Default cost is 6.
- FDDI—Default cost is 1.
- X25—Default cost is 5208.
- Asynchronous—Default cost is 10,000.
- ATM— Default cost is 1.The dynamic cost is calculated using the following formula:

  L2L3API

Where the metric calculations are

S1 = ipv6 ospf dynamic weight throughput
S2 = ipv6 ospf dynamic weight resources
S3 = ipv6 ospf dynamic weight latency
S4 = ipv6 ospf dynamic weight L2 factor
OC = standard cost of a non-VMI route

Throughput = (current-data-rate)/(maximum-data-rate)

Router-dynamic cost= OC + (S1) + (S2) + (S3) + (S4)

For a dynamic cost to have the same cost as a default cost, all parameters must equal zero.

Each Layer 2 feedback can contribute a cost in the range of 0 to 65535. To tune down this cost range, use the optional **weight** keyword in conjunction with the **throughput**, **resources**, **latency**, or **L2-factor** keyword. Each of these weights has a default value of 100% and can be configured in the range from 0 to 100. When 0 is configured for a specific weight, that weight does not contribute to the OSPFv3 cost.

Because cost components can change rapidly, you may need to dampen the amount of changes in order to reduce network-wide churn. Use the optional **hysteresis** keyword with the **threshold** *threshold-value* keyword and argument to set a cost change threshold. Any cost change below this threshold is ignored.

Examples

Interface Cost Example

The following example sets the interface cost value to 65:

```
ipv6 ospf cost 65
```

VMI Interface Cost Example

The following example sets the interface cost value for a VMI interface:

```
interface vmi 0
ipv6 ospf cost dynamic hysteresis threshold 30
ipv6 ospf cost dynamic weight throughput 75
ipv6 ospf cost dynamic weight resources 70
ipv6 ospf cost dynamic weight latency 80
ipv6 ospf cost dynamic weight L2-factor 10
```

Related Commands

Command	Description
interface vmi	Creates a virtual multipoint interface that can be configured and applied dynamically.
ipv6 ospf neighbor	Configures OSPFv3 routers interconnecting to nonbroadcast networks.
ospfv3 cost	Explicitly specifies the cost of sending a packet on an interface.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

ipv6 ospf database-filter all out

To filter outgoing link-state advertisements (LSAs) to an Open Shortest Path First version 3 (OSPFv3) interface, use the **ipv6 ospf database-filter all out** command in interface configuration mode. To restore the forwarding of LSAs to the interface, use the **no** form of this command.

ipv6 ospf database-filter all out

no ipv6 ospf database-filter all out

Syntax Description

This command has no arguments or keywords.

Command Default

All outgoing LSAs are flooded to the interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)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.
15.1(3)S	Use of the **ospfv3 database-filter** command can affect the **ipv6 ospf database-filter all out** command.
Cisco IOS XE Release 3.4S	Use of the **ospfv3 database-filter** command can affect the **ipv6 ospf database-filter all out** command.
15.2(1)T	Use of the **ospfv3 database-filter** command can affect the **ipv6 ospf database-filter all out** command.

Usage Guidelines

This command performs the same function that the **neighbor database-filter** command performs on a neighbor basis.

Examples

The following example prevents flooding of OSPFv3 LSAs to broadcast, nonbroadcast, or point-to-point networks reachable through Ethernet interface 0:

```
interface ethernet 0
 ipv6 ospf database-filter all out
```

Related Commands

ospfv3 database-filter	Filters outgoing LSAs to an OSPFv3 interface
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

ipv6 ospf dead-interval

To set the time period for which hello packets must not be seen before neighbors declare the router down, use the **ipv6 ospf dead-interval** command in interface configuration mode. To return to the default time, use the **no** form of this command.

ipv6 ospf dead-interval *seconds*

no ipv6 ospf dead-interval

Syntax Description

seconds	Specifies the interval (in seconds). The value must be the same for all nodes on the network.

Command Default

Four times the interval set by the **ipv6 ospf hello-interval** command

Command Modes

Interface configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)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.
15.1(3)S	Use of the **ospfv3 dead-interval** command can affect the **ipv6 ospf dead-interval** command.
Cisco IOS XE Release 3.4S	Use of the **ospfv3 dead-interval** command can affect the **ipv6 ospf dead-interval** command.
15.2(1)T	Use of the **ospfv3 dead-interval** command can affect the **ipv6 ospf dead-interval** command.

Usage Guidelines

The interval is advertised in router hello packets. This value must be the same for all routers and access servers on a specific network.

When the **ospfv3 dead-interval** command is configured with the *process-id* argument, it overwrites the **ipv6 dead-interval** configuration if OSPFv3 was attached to the interface using the **ipv6 ospf area** command.

Examples

The following example sets the Open Shortest Path First version 3 (OSPFv3) dead interval to 60 seconds:

```
interface ethernet 1
 ipv6 ospf dead-interval 60
```

Related Commands

Command	Description
ipv6 ospf hello-interval	Specifies the interval between hello packets that the Cisco IOS software sends on the interface.
ospfv3 dead-interval	Sets the time period for which hello packets must not be seen before neighbors declare the router down.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

ipv6 ospf demand-circuit

To configure Open Shortest Path First version 3 (OSPF) to treat the interface as an OSPFv3 demand circuit, use the **ipv6 ospf demand-circuit** command in interface configuration mode. To remove the demand circuit designation from the interface, use the **no** form of this command.

ipv6 ospf demand-circuit

no ipv6 ospf demand-circuit

Syntax Description

This command has no arguments or keywords.

Command Default

The circuit is not a demand circuit.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)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.
15.1(3)S	Use of the **ospfv3 demand-circuit** command can affect the **ipv6 ospf demand-circuit** command.
Cisco IOS XE Release 3.4S	Use of the **ospfv3 demand-circuit** command can affect the **ipv6 ospf demand-circuit** command.
15.2(1)T	Use of the **ospfv3 demand-circuit** command can affect the **ipv6 ospf demand-circuit** command.

Usage Guidelines

When the **ospfv3 demand-circuit** command is configured with the *process-id* argument, it overwrites the **ipv6 ospf demand-circuit** configuration if OSPFv3 was attached to the interface using the **ipv6 ospf area** command.

On point-to-point interfaces, only one end of the demand circuit must be configured with this command. Periodic hello messages are suppressed and periodic refreshes of link-state advertisements (LSAs) do not flood the demand circuit. This command allows the underlying data link layer to be closed when the topology is stable. In point-to-multipoint topology, only the multipoint end must configured with this command.

Examples

The following example sets the configuration for an ISDN on-demand circuit:

```
interface BRI0
 ipv6 ospf 1 area 1
 ipv6 ospf demand-circuit
```

Related Commands

ospfv3 demand-circuit	Configures OSPFv3 to treat the interface as an OSPFv3 demand circuit.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

ipv6 ospf encryption

To specify the encryption type for an interface, use the **ipv6 ospf encryption** command in interface configuration mode. To remove the encryption type from an interface, use the **no** form of this command.

ipv6 ospf encryption {**ipsec spi** *spi* **esp** *encryption-algorithm* [[*key-encryption-type*] *key*] *authentication-algorithm* [*key-encryption-type*] *key* | **null**}

no ipv6 ospf encryption ipsec spi *spi*

Syntax Description

ipsec	IP Security (IPSec).
spi *spi*	Security policy index (SPI) value. The *spi* value must be a number from 256 to 4294967295.
esp	Encapsulating security payload (ESP).
encryption-algorithm	Encryption algorithm to be used with ESP. The values can be any of the following: • **aes-cdc**—Enables AES-CDC encryption. • **3des**—Enables 3DES encryption. • **des**—Enables DES encryption. • **null**—ESP with no encryption.
key-encryption-type	(Optional) One of two values can be entered: • **0**—The key is not encrypted. • **7**—The key is encrypted.
key	(Optional) Number used in the calculation of the message digest. The number is 32 hex digits (16 bytes) long. The size of the key depends on the encryption algorithm used. Some algorithms, such as AES-CDC, allow the user to choose the size of the key.
authentication-algorithm	Encryption authentication algorithm to be used. The values can be one of the following: • **md5**—Enables message digest 5 (MD5). • **sha1**—Enables SHA-1.
null	Overrides area encryption.

Command Default

Authentication and encryption are not configured on an interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.
15.1(3)S	Use of the **ospfv3 encryption** command can affect the **ipv6 ospf encryption** command.

Release	Modification
Cisco IOS XE Release 3.4S	Use of the **ospfv3 encryption** command can affect the **ipv6 ospf encryption** command.
15.2(1)T	Use of the **ospfv3 encryption** command can affect the **ipv6 ospf encryption** command.

Usage Guidelines

When the **ipv6 ospf encryption** command is enabled, both authentication and encryption are enabled.

The user needs to ensure that the same policy (the SPI and the key) is configured on all of the interfaces on the link. SPI values may automatically be used by other client applications, such as tunnels.

The policy database is common to all client applications on a box. This means that two IPSec clients, such as Open Shortest Path First version 3 (OSPFv3) and a tunnel, cannot use the same SPI. Additionally, an SPI can be used only in one policy.

The **null** keyword is used to override existing area encryption. If area encryption is not configured, then it is not necessary to configure the interface with the **ipv6 ospf encryption null** command.

Examples

The following example specifies the encryption type for Ethernet interface 0/0. The IPSec SPI value is 1001, ESP is used with no encryption, and the authentication algorithm is SHA-1.

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 ospf encryption ipsec spi 1001 esp null sha1
123456789A123456789B123456789C123456789D
```

Related Commands

Command	Description
area authentication	Enables authentication for an OSPFv3 area.
area encryption	Enables encryption for an OSPFv3 area.
area virtual-link authentication	Enables authentication for virtual links in an OSPFv3 area.
ipv6 ospf authentication	Specifies the authentication type for an interface.
ospfv3 encryption	Specifies the encryption type for an interface.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

ipv6 ospf flood-reduction

To suppress the unnecessary flooding of link-state advertisements (LSAs) in stable topologies, use the **ipv6 ospf flood-reduction** command in interface configuration mode. To disable this feature, use the **no** form of this command.

ipv6 ospf flood-reduction

no ipv6 ospf flood-reduction

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)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.
15.1(3)S	Use of the **ospfv3 flood-reduction** command can affect the **ipv6 ospf flood-reduction** command.
Cisco IOS XE Release 3.4S	Use of the **ospfv3 flood-reduction** command can affect the **ipv6 ospf flood-reduction** command.
15.2(1)T	Use of the **ospfv3 flood-reduction** command can affect the **ipv6 ospf flood-reduction** command.

Usage Guidelines

When the **ospfv3 flood-reduction** command is configured with the *process-id* argument, it overwrites the **ipv6 ospf flood-reduction** configuration if OSPFv3 was attached to the interface using the **ipv6 ospf flood-reduction** command.

All routers supporting the Open Shortest Path First version 3 (OSPFv3) demand circuit are compatible and can interact with routers supporting flooding reduction.

Examples

The following example suppresses the flooding of unnecessary LSAs on serial interface 0:

```
interface serial 0
 ipv6 ospf flood-reduction
```

Related Commands

Command	Description
ospfv3 flood-reduction	Suppresses the unnecessary flooding of LSAs in stable topologies.
show ipv6 ospf interface	Displays OSPFv3-related interface information.
show ipv6 ospf neighbor	Displays OSPFv3-neighbor information on a per-interface basis.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

ipv6 ospf hello-interval

To specify the interval between hello packets that the Cisco IOS software sends on the Open Shortest Path First version 3 (OSPFv3) interface, use the **ipv6 ospf hello-interval** command in interface configuration mode. To return to the default time, use the **no** form of this command.

ipv6 ospf hello-interval *seconds*

no ipv6 ospf hello-interval

Syntax Description

seconds	Specifies the interval (in seconds). The value must be the same for all nodes on a specific network.

Command Default

The default interval is 10 seconds when using Ethernet and 30 seconds when using nonbroadcast.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)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.
15.1(3)S	Use of the **ospfv3 mtu-ignore** command can affect the **ipv6 ospf mtu-ignore** command.
Cisco IOS XE Release 3.4S	Use of the **ospfv3 mtu-ignore** command can affect the **ipv6 ospf mtu-ignore** command.
15.2(1)T	Use of the **ospfv3 mtu-ignore** command can affect the **ipv6 ospf mtu-ignore** command.

Usage Guidelines

When the **ospfv3 hello-interval** command is configured with the *process-id* argument, it overwrites the **ipv6 ospf hello-interval** configuration if OSPFv3 was attached to the interface using the **ipv6 ospf area** command.

This value is advertised in the hello packets. The shorter the hello interval, the earlier topological changes will be detected, but more routing traffic will ensue. This value must be the same for all routers and access servers on a specific network.

Examples

The following example sets the interval between hello packets to 15 seconds:

```
interface ethernet 1
```

```
ipv6 ospf hello-interval 15
```

Related Commands

Command	Description
ipv6 ospf dead-interval	Sets the time period for which hello packets must not have been seen before neighbors declare the router down.
ospfv3 hello-interval	Specifies the interval between hello packets that the Cisco IOS software sends on the interface.

ipv6 ospf mtu-ignore

To disable Open Shortest Path First version 3 (OSPFv3) maximum transmission unit (MTU) mismatch detection on receiving database descriptor (DBD) packets, use the **ipv6 ospf mtu-ignore** command in interface configuration mode. To reset to default, use the **no** form of this command.

ipv6 ospf mtu-ignore

no ipv6 ospf mtu-ignore

Syntax Description

This command has no arguments or keywords.

Command Default

OSPFv3 MTU mismatch detection is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)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.
15.1(3)S	Use of the **ospfv3 mtu-ignore** command can affect the **ipv6 ospf mtu-ignore** command.
Cisco IOS XE Release 3.4S	Use of the **ospfv3 mtu-ignore** command can affect the **ipv6 ospf mtu-ignore** command.
15.2(1)T	Use of the **ospfv3 mtu-ignore** command can affect the **ipv6 ospf mtu-ignore** command.

Usage Guidelines

When the **ospfv3 mtu-ignore** command is configured with the *process-id* argument, it overwrites the **ipv6 ospf mtu-ignore** configuration if OSPFv3 was attached to the interface using the **ipv6 ospf area** command.

OSPFv3 checks whether neighbors are using the same MTU on a common interface. This check is performed when neighbors exchange DBD packets. If the receiving MTU in the DBD packet is higher then the IP MTU configured on the incoming interface, OSPFv3 adjacency will not be established.

Examples

The following example disables MTU mismatch detection on receiving DBD packets:

```
interface serial 0/0
 ipv6 ospf mtu-ignore
```

Related Commands

Command	Description
ospfv3 mtu-ignore	Disables OSPFv3 MTU mismatch detection on receiving DBD packets.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

ipv6 ospf name-lookup

To display Open Shortest Path First (OSPF) router IDs as Domain Naming System (DNS) names, use the **ipv6 ospf name-lookup** command in global configuration mode. To stop displaying OSPF router IDs as DNS names, use the **no** form of this command.

ipv6 ospf name-lookup

no ipv6 ospf name-lookup

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default

Command Modes

Global configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)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.

Usage Guidelines

This command makes it easier to identify a router because the router is displayed by name rather than by its router ID or neighbor ID.

Examples

The following example configures OSPF to look up DNS names for use in all OSPF show EXEC command displays:

```
ipv6 ospf name-lookup
```

ipv6 ospf neighbor

To configure Open Shortest Path First (OSPF) routers interconnecting to nonbroadcast networks, use the **ipv6 ospf neighbor** command in interface configuration mode. To remove a configuration, use the **no** form of this command.

ipv6 ospf neighbor *ipv6-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*] [**database-filter all out**]

no ipv6 ospf neighbor *ipv6-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*] [**database-filter all out**]

Syntax Description

ipv6-address	Link-local IPv6 address of the neighbor. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
priority *number*	(Optional) A number that indicates the router priority value of the nonbroadcast neighbor associated with the IPv6 prefix specified. The default is 0.
poll-interval *seconds*	(Optional) A number value that represents the poll interval time (in seconds). RFC 2328 recommends that this value be much larger than the hello interval. The default is 120 seconds (2 minutes). This keyword does not apply to point-to-multipoint interfaces.
cost *number*	(Optional) Assigns a cost to the neighbor, in the form of an integer from 1 to 65535. Neighbors with no specific cost configured will assume the cost of the interface, based on the **ipv6 ospf cost** command.
database-filter all out	(Optional) Filters outgoing link-state advertisements (LSAs) to an OSPF neighbor.

Command Default

No configuration is specified.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)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.

Usage Guidelines

X.25 and Frame Relay provide an optional broadcast capability that can be configured in the map to allow OSPF to run as a broadcast network. At the OSPF level you can configure the router as a broadcast network.

One neighbor entry must be included in the Cisco IOS software configuration for each known nonbroadcast network neighbor. The neighbor address must be a link-local address of the neighbor.

If a neighboring router has become inactive (hello packets have not been seen for the Router Dead Interval period), hello packets may need to be sent to the dead neighbor. These hello packets will be sent at a reduced rate called *Poll Interval*.

When the router first starts up, it sends only hello packets to those routers with nonzero priority, that is, routers that are eligible to become designated routers (DRs) and backup designated routers (BDRs). After the DR and BDR are selected, the DR and BDR will then start sending hello packets to all neighbors in order to form adjacencies.

The **priority** keyword does not apply to point-to-multipoint interfaces. For point-to-multipoint interfaces, the **cost** keyword and the *number* argument are the only options that are applicable. The **cost** keyword does not apply to nonbroadcast multiaccess (NBMA) networks.

Examples

The following example configures an OSPF neighboring router:

```
ipv6 ospf neighbor FE80::A8BB:CCFF:FE00:C01
```

ipv6 ospf network

To configure the Open Shortest Path First version 3 (OSPFv3) network type to a type other than the default for a given medium, use the **ipv6 ospf network** command in interface configuration mode. To return to the default type, use the **no** form of this command.

ipv6 ospf network {**broadcast** | **non-broadcast** | {**point-to-multipoint** [**non-broadcast**] | **point-to-point**}}

no ipv6 ospf network

Syntax Description

broadcast	Sets the network type to broadcast.
non-broadcast	Sets the network type to nonbroadcast multiaccess (NBMA).
point-to-multipoint [**non-broadcast**]	Sets the network type to point-to-multipoint. The optional **non-broadcast** keyword sets the point-to-multipoint network to be nonbroadcast. If you use the **non-broadcast** keyword, the **neighbor** command is required.
point-to-point	Sets the network type to point-to-point.

Command Default

Default depends on the network type.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)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.
12.4(15)XF	The **point-to-multipoint** keyword was added to support the Virtual Multipoint Interfaces (VMI) and Mobile Adhoc Networking.
12.4(15)T	This command was integrated into Cisco IOS 12.4(15)T.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
15.1(3)S	Use of the **ospfv3 network** command can affect the **ipv6 ospf network** command.
Cisco IOS XE Release 3.4S	Use of the **ospfv3 network** command can affect the **ipv6 ospf network** command.
15.2(1)T	Use of the **ospfv3 network** command can affect the **ipv6 ospf network** command.

Usage Guidelines

When the **ospfv3 network** command is configured with the *process-id* argument, it overwrites the **ipv6 ospf network** configuration if OSPFv3 was attached to the interface using the **ipv6 ospf area** command.

NBMA Networks

Using this feature, you can configure broadcast networks as NBMA networks when, for example, routers in your network do not support multicast addressing. You can also configure NBMA networks (such as X.25, Frame Relay, and Switched Multimegabit Data Service [SMDS]) as broadcast networks. This feature saves you from needing to configure neighbors.

Configuring NBMA networks as either broadcast or nonbroadcast assumes that there are virtual circuits from every router to every router or fully meshed networks. However, the assumption is not true for other configurations, such as for a partially meshed network. In these cases, you can configure the OSPFv3 network type as a point-to-multipoint network. Routing between two routers that are not directly connected will go through the router that has virtual circuits to both routers. You need not configure neighbors when using this feature.

Point-to-Multipoint Networks

OSPFv3 for IPv6 has two features related to point-to-multipoint networks. One feature applies to broadcast networks; the other feature applies to nonbroadcast networks:

- On point-to-multipoint, broadcast networks, you can use the **neighbor** command, and you must specify a cost to that neighbor.
- On point-to-multipoint, nonbroadcast networks, you must use the **neighbor** command to identify neighbors. Assigning a cost to a neighbor is optional.

Examples

OSPFv3 Network as Broadcast Network Example

The following example sets your OSPFv3 network as a broadcast network:

```
interface serial 0
 ipv6 enable
 ipv6 ospf 1 area 0
 ipv6 ospf network broadcast
 encapsulation frame-relay
```

OSPFv3 Point-to-Multipoint Network with Broadcast Example

The following example illustrates a point-to-multipoint network with broadcast:

```
interface serial 0
 ipv6 enable
 ipv6 ospf 1 area 0
 encapsulation frame-relay
 ipv6 ospf cost 100
 ipv6 ospf network point-to-multipoint
 frame-relay map ipv6 2001:0DB1::A8BB:CCFF:FE00:C01 broadcast
 frame-relay map ipv6 2001:0DB1B:CCFF:FE00:C02 broadcast
 frame-relay local-dlci 200
 ipv6 ospf neighbor 2001:0DB1B:CCFF:FE00:C01
 ipv6 ospf neighbor2001:0DB1B:CCFF:FE00:C02
```

Related Commands

Command	Description
frame-relay map	Defines mapping between a destination protocol address and the DLCI used to connect to the destination address.
ipv6 ospf neighbor	Configures OSPFv3 routers interconnecting to nonbroadcast networks.
ospfv3 network	Configures an OSPFv3 network type to a type other than the default for a given medium.
x25 map	Sets up the LAN protocols-to-remote host mapping.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

ipv6 ospf priority

To set the router priority, which helps determine the designated router for this network, use the **ipv6 ospf priority** command in interface configuration mode. To return to the default value, use the **no** form of this command.

ipv6 ospf priority *number-value*

no ipv6 ospf priority *number-value*

Syntax Description

number-value	A number value that specifies the priority of the router. The range is from 0 to 255.

Command Default

The router priority is 1.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)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.
15.1(3)S	Use of the **ospfv3 priority** command can affect the **ipv6 ospf priority** command.
Cisco IOS XE Release 3.4S	Use of the **ospfv3 priority** command can affect the **ipv6 ospf priority** command.
15.2(1)T	Use of the **ospfv3 priority** command can affect the **ipv6 ospf priority** command.

Usage Guidelines

When the **ospfv3 priority** command is configured with the *process-id* argument, it overwrites the **ipv6 ospf priority** configuration if OSPFv3 was attached to the interface using the **ipv6 ospf area** command.

When two routers attached to a network both attempt to become the designated router, the one with the higher router priority takes precedence. If there is a tie, the router with the higher router ID takes precedence. A router with a router priority set to zero is ineligible to become the designated router or backup designated router. Router priority is configured only for interfaces to multiaccess networks (in other words, not to point-to-point networks).

This priority value is used when you configure Open Shortest Path First version 3 (OSPFv3) for nonbroadcast networks using the **ipv6 ospf neighbor** command.

Examples

The following example sets the router priority value to 4:

```
interface ethernet 0
 ipv6 ospf priority 4
```

Related Commands

Command	Description
ipv6 ospf network	Configures the OSPFv3 network type to a type other than the default for a given medium.
ipv6 ospf neighbor	Configures OSPFv3 routers interconnecting to nonbroadcast networks.
ospfv3 priority	Sets the router priority, which helps determine the designated router for this network.

ipv6 ospf retransmit-interval

To specify the time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the Open Shortest Path First version 3 (OSPFv3) interface, use the **ipv6 ospf retransmit-interval** command in interface configuration mode. To return to the default value, use the **no** form of this command.

ipv6 ospf retransmit-interval *seconds*

no ipv6 ospf retransmit-interval

Syntax Description

seconds	Time (in seconds) between retransmissions. It must be greater than the expected round-trip delay between any two routers on the attached network. The range is from 1 to 65535 seconds. The default is 5 seconds.

Command Default

The default is 5 seconds.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)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.
15.1(3)S	Use of the **ospfv3 retransmit-interval** command can affect the **ipv6 ospf retransmit-interval** command.
Cisco IOS XE Release 3.4S	Use of the **ospfv3 retransmit-interval** command can affect the **ipv6 ospf retransmit-interval** command.
15.2(1)T	Use of the **ospfv3 retransmit-interval** command can affect the **ipv6 ospf retransmit-interval** command.

Usage Guidelines

When the **ospfv3 retransmit-interval** command is configured with the *process-id* argument, it overwrites the **ipv6 ospf retransmit-interval** configuration if OSPFv3 was attached to the interface using the **ipv6 ospf area** command.

When a router sends an LSA to its neighbor, it keeps the LSA until it receives back the acknowledgment message. If the router receives no acknowledgment, it will resend the LSA.

The setting of this parameter should be conservative, or needless retransmission will result. The value should be larger for serial lines and virtual links.

Examples

The following example sets the retransmit interval value to 8 seconds:

```
interface ethernet 2
 ipv6 ospf retransmit-interval 8
```

Related Commands

Command	Description
ospfv3 retransmit-interval	Specifies the time between LSA retransmissions for adjacencies belonging to the interface.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

ipv6 ospf transmit-delay

To set the estimated time required to send a link-state update packet on the Open Shortest Path First version 3 (OSPFv3) interface, use the **ip ospf transmit-delay** command in interface configuration mode. To return to the default value, use the **no** form of this command.

ipv6 ospf transmit-delay *seconds*

no ipv6 ospf transmit-delay

Syntax Description

seconds	Time (in seconds) required to send a link-state update. The range is from 1 to 65535 seconds. The default is 1 second.

Command Default

The default is 1 second.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)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.
15.1(3)S	Use of the **ospfv3 transmit-delay** command can affect the **ipv6 ospf transmit-delay** command.
Cisco IOS XE Release 3.4S	Use of the **ospfv3 transmit-delay** command can affect the **ipv6 ospf transmit-delay** command.
15.2(1)T	Use of the **ospfv3 transmit-delay** command can affect the **ipv6 ospf transmit-delay** command.

Usage Guidelines

When the **ospfv3 transmit-delay** command is configured with the *process-id* argument, it overwrites the **ipv6 ospf transmit-delay** configuration if OSPFv3 was attached to the interface using the **ipv6 ospf area** command.

Link-state advertisements (LSAs) in the update packet must have their ages incremented by the amount specified in the *seconds* argument before transmission. The value assigned should take into account the transmission and propagation delays for the interface.

If the delay is not added before transmission over a link, the time in which the LSA propagates over the link is not considered. This setting has more significance on very low-speed links.

Examples

The following example sets the retransmit delay value to 3 seconds:

```
interface ethernet 0
 ipv6 ospf transmit-delay 3
```

Related Commands

Command	Description
ospfv3 transmit-delay	Sets the estimated time required to send a link-state update packet on the interface.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

ipv6 pim

To reenable IPv6 Protocol Independent Multicast (PIM) on a specified interface, use the **ipv6 pim** command in interface configuration mode. To disable PIM on a specified interface, use the **no** form of the command.

ipv6 pim

no ipv6 pim

Syntax Description

This command has no arguments or keywords.

Command Default

PIM is automatically enabled on every interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
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.
12.2(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

After a user has enabled the **ipv6 multicast-routing** command, PIM is enabled to run on every interface. Because PIM is enabled on every interface by default, use the **no** form of the **ipv6 pim** command to disable PIM on a specified interface. When PIM is disabled on an interface, it does not react to any host membership notifications from the Multicast Listener Discovery (MLD) protocol.

Examples

The following example turns off PIM on Fast Ethernet interface 1/0:

```
Router(config)# interface FastEthernet 1/0
Router(config-if)# no ipv6 pim
```

Related Commands

Command	Description
ipv6 multicast-routing	Enables multicast routing using PIM and MLD on all IPv6-enabled interfaces of the router and enables multicast forwarding.

ipv6 pim accept-register

To accept or reject registers at the rendezvous point (RP), use the **ipv6 pim accept-register** command in global configuration mode. To return to the default value, use the **no** form of this command.

ipv6 pim [**vrf** *vrf-name*] **accept-register** {**list** *access-list* | **route-map** *map-name*}

no ipv6 pim [**vrf** *vrf-name*] **accept-register** {**list** *access-list* | **route-map** *map-name*}

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
list *access-list*	Defines the access list name.
route-map *map-name*	Defines the route map.

Command Default

All sources are accepted at the RP.

Command Modes

Global configuration

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
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.
12.2(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(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

Use the **ipv6 pim accept-register** command to configure a named access list or route map with match attributes. When the permit conditions as defined by the *access-list* and *map-name* arguments are met, the register message is accepted. Otherwise, the register message is not accepted, and an immediate register-stop message is returned to the encapsulating designated router.

Examples

The following example shows how to filter on all sources that do not have a local multicast Border Gateway Protocol (BGP) prefix:

```
ipv6 pim accept-register route-map reg-filter
route-map reg-filter permit 20
 match as-path 101
ip as-path access-list 101 permit
```

ipv6 pim bsr candidate rp

To configure the candidate rendezvous point (RP) to send Protocol Independent Multicast (PIM) RP advertisements to the bootstrap router (BSR), use the **ipv6 pim bsr candidate rp** command in global configuration mode. To disable PIM RP advertisements to the BSR, use the **no** form of this command.

ipv6 pim [**vrf** *vrf-name*] **bsr candidate rp** *ipv6-address* [**group-list** *access-list-name*] [**priority** *priority-value*] [**interval** *seconds*] [**scope** *scope-value*] [**bidir**]

no ipv6 pim [**vrf** *vrf-name*] **bsr candidate rp** *ipv6-address* [**group-list** *access-list-name*] [**priority** *priority-value*] [**interval** *seconds*] [**scope** *scope-value*] [**bidir**]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
ipv6-address	The IPv6 address of the router to be advertised as the candidate RP (C-RP). This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
group-list	(Optional) List of group prefixes. When the **bidir** keyword is not enabled, the **group-list** keyword with the *access-list-name* argument is advertised in the sparse range. If no access list is specified, all valid multicast nonsource-specific multicast (SSM) address ranges are advertised in association with the specified RP address.
access-list-name	(Optional) Name of the IPv6 access list containing group prefixes that will be advertised in association with the RP address. Names cannot contain a space or quotation mark, or begin with a numeral. When the **bidir** keyword is not enabled, the **group-list** keyword with the *access-list-name* argument is advertised in the sparse range. If the access list contains any group address ranges that overlap the assigned SSM group address range (FF3x::/96), a warning message is displayed, and the overlapping address ranges are ignored.
priority	(Optional) Priority of the candidate BSR.
priority-value	(Optional) Integer from 0 through 192 that specifies the priority. The RP with the higher priority is preferred. If the priority values are the same, the router with the higher IPv6 address is the RP. The default value is 192.
interval	(Optional) Configures the C-RP advertisement interval.
seconds	(Optional) Advertisement interval in number of seconds.
scope	(Optional) Router advertises itself as the C-RP only to the BSR for the specified scope.
scope-value	(Optional) Integer from 3 through 15 that specifies the scope.
bidir	(Optional) Router advertises itself as the C-RP for the **group-list** *access-list-name* in the bidirectional range.

Command Default

Router is not enabled as a candidate RP.
If no scope is configured, all scopes are advertised.

Command Modes Global configuration

Command History

Release	Modification
12.0(28)S	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(11)T	This command was integrated into Cisco IOS Release 12.3(11)T.
12.4	The **scope** keyword and *scope-value* argument are no longer available in syntax.
12.4(2)T	This command was integrated into Cisco IOS Release 12.4(2)T.
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.
12.2(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.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines Use the **ipv6 pim bsr candidate rp** command to send PIM RP advertisements to the BSR.

The group prefixes defined by the *access-list-name* argument will also be advertised in association with the RP address. If a group prefix in the access list is denied, it will not be included in the C-RP advertisement.

If the **priority** *priority-value* keyword and argument are specified, then the router will announce itself to be a candidate RP with the specified priority.

If the **scope** keyword is used, the router advertises itself as the C-RP only to the BSR for the specified scope. If the **group-list** keyword is specified along with the scope, then only prefixes in the *access-list-name* argument with the same scope as the scope configured will be advertised. If no scope is configured, all scopes are advertised.

Examples The following example configures the router with the IPv6 address 2001:0DB8:3000:3000::42 to be advertised as the candidate RP, with a priority of 0:

```
Router(config)# ipv6 pim bsr candidate rp 2001:0DB8:3000:3000::42 priority 0
```

The following example configures the router with the IPv6 address 2001:0DB8:1:1:1 as the candidate RP for scope 6 for the group ranges specified in the access list named list1:

```
Router(config)# ipv6 pim bsr candidate rp 2001:0DB8:1:1:1 group-list list1 scope 6
```

Related Commands

Command	Description
ipv6 pim bsr candidate bsr	Configures a router as a candidate BSR.
ipv6 pim bsr border	Configures a border for all BSMs of any scope.

ipv6 pim bsr border

To configure a border for all bootstrap message (BSMs) of any scope on a specified interface, use the **ipv6 pim bsr border** command in interface configuration mode. To remove the border, use the **no** form of this command.

ipv6 pim bsr border

no ipv6 pim bsr border

Syntax Description

This command has no argument or keywords.

Command Default

No border is configured.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(28)S	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(11)T	This command was integrated into Cisco IOS Release 12.3(11)T.
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.
12.2(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 **ipv6 pim bsr border** command is used to configure a border to all global and scoped BSMs. The command filters incoming or outgoing BSMs, preventing the BSMs from being forwarded or accepted on the interface on which the **ipv6 pim bsr border** command is configured.

Examples

The following example configures a BSR border on Ethernet interface 1/0:

```
Router(config)# interface Ethernet1/0
 Router(config-if)# ipv6 pim bsr border
 Router(config-if)# end

Router# show running-config interface e1/0

 Building configuration...

 Current configuration :206 bytes
 !
 interface Ethernet1/0
```

```
ipv6 address 2:2:2::2/64
ipv6 enable
ipv6 rip test enable
ipv6 pim bsr border
no cdp enable
end
```

Related Commands

Command	Description
ipv6 pim bsr candidate bsr	Configures a router as a candidate BSR.
ipv6 pim bsr candidate rp	Sends PIM RP advertisements to the BSR.

ipv6 pim bsr candidate bsr

To configure a router to be a candidate bootstrap router (BSR), use the **ipv6 pim bsr candidate bsr** command in global configuration mode. To remove this router as a candidate BSR, use the **no** form of this command.

ipv6 pim [**vrf** *vrf-name*] **bsr candidate bsr** *ipv6-address* [*hash-mask-length*] [**priority** *priority-value*]

no ipv6 pim [**vrf** *vrf-name*] **bsr candidate bsr** *ipv6-address* [*hash-mask-length*] [**priority** *priority-value*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
ipv6-address	The IPv6 address of the router to be configured as a candidate BSR. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
hash-mask-length	(Optional) The length (in bits) of the mask to use in the BSR hash function. The default value is 126.
priority	(Optional) Priority of the candidate BSR.
priority-value	(Optional) Integer from 0 through 192. The BSR with the larger priority is preferred. If the priority values are the same, the router with the larger IPv6 address is the BSR. The default value is 0.
scope	(Optional) BSR will originate bootstrap messages (BSMs), including the group range associated with the scope, and accept candidate RP (C-RP) announcements only if they are for groups that belong to the given scope.

Command Default

Router is not enabled as a BSR.

Command Modes

Global configuration

Command History

Release	Modification
12.0(28)S	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(11)T	This command was integrated into Cisco IOS Release 12.3(11)T.
12.4	The **scope** keyword and *scope-value* argument are no longer available in syntax.
12.4(2)T	This command was integrated into Cisco IOS Release 12.4(2)T.
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.
12.2(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(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

The **ipv6 pim bsr candidate bsr** command is used to configure a router as a candidate BSR. When a router is configured, it will participate in BSR election. If elected BSR, this router will periodically originate BSR messages advertising the group-to-RP mappings it has learned through candidate-RP-advertisement messages.

If the **scope** keyword is enabled, the BSR will originate BSMs, including the group range associated with the scope, and accept C-RP announcements only if they are for groups that belong to the given scope. If no scope is configured, all scopes are used.

Examples

The following example configures the router with the IPv6 address 2001:0DB8:3000:3000::42 as the candidate BSR, with a hash mask length of 124 and a priority of 10:

```
ipv6 pim bsr candidate bsr 2001:0DB8:3000:3000::42 124 priority 10
```

Related Commands

Command	Description
ipv6 pim bsr border	Configures a border for all bootstrap message BSMs of any scope.
ipv6 pim bsr candidate rp	Sends PIM RP advertisements to the BSR.

ipv6 pim bsr candidate rp

To configure the candidate rendezvous point (RP) to send Protocol Independent Multicast (PIM) RP advertisements to the bootstrap router (BSR), use the **ipv6 pim bsr candidate rp** command in global configuration mode. To disable PIM RP advertisements to the BSR, use the **no** form of this command.

ipv6 pim [**vrf** *vrf-name*] **bsr candidate rp** *ipv6-address* [**group-list** *access-list-name*] [**priority** *priority-value*] [**interval** *seconds*] [**scope** *scope-value*] [**bidir**]

no ipv6 pim [**vrf** *vrf-name*] **bsr candidate rp** *ipv6-address* [**group-list** *access-list-name*] [**priority** *priority-value*] [**interval** *seconds*] [**scope** *scope-value*] [**bidir**]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
ipv6-address	The IPv6 address of the router to be advertised as the candidate RP (C-RP). This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
group-list	(Optional) List of group prefixes. When the **bidir** keyword is not enabled, the **group-list** keyword with the *access-list-name* argument is advertised in the sparse range. If no access list is specified, all valid multicast nonsource-specific multicast (SSM) address ranges are advertised in association with the specified RP address.
access-list-name	(Optional) Name of the IPv6 access list containing group prefixes that will be advertised in association with the RP address. Names cannot contain a space or quotation mark, or begin with a numeral. When the **bidir** keyword is not enabled, the **group-list** keyword with the *access-list-name* argument is advertised in the sparse range. If the access list contains any group address ranges that overlap the assigned SSM group address range (FF3x::/96), a warning message is displayed, and the overlapping address ranges are ignored.
priority	(Optional) Priority of the candidate BSR.
priority-value	(Optional) Integer from 0 through 192 that specifies the priority. The RP with the higher priority is preferred. If the priority values are the same, the router with the higher IPv6 address is the RP. The default value is 192.
interval	(Optional) Configures the C-RP advertisement interval.
seconds	(Optional) Advertisement interval in number of seconds.
scope	(Optional) Router advertises itself as the C-RP only to the BSR for the specified scope.
scope-value	(Optional) Integer from 3 through 15 that specifies the scope.
bidir	(Optional) Router advertises itself as the C-RP for the **group-list** *access-list-name* in the bidirectional range.

Command Default

Router is not enabled as a candidate RP.
If no scope is configured, all scopes are advertised.

Command Modes Global configuration

Command History

Release	Modification
12.0(28)S	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(11)T	This command was integrated into Cisco IOS Release 12.3(11)T.
12.4	The **scope** keyword and *scope-value* argument are no longer available in syntax.
12.4(2)T	This command was integrated into Cisco IOS Release 12.4(2)T.
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.
12.2(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.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines Use the **ipv6 pim bsr candidate rp** command to send PIM RP advertisements to the BSR.

The group prefixes defined by the *access-list-name* argument will also be advertised in association with the RP address. If a group prefix in the access list is denied, it will not be included in the C-RP advertisement.

If the **priority** *priority-value* keyword and argument are specified, then the router will announce itself to be a candidate RP with the specified priority.

If the **scope** keyword is used, the router advertises itself as the C-RP only to the BSR for the specified scope. If the **group-list** keyword is specified along with the scope, then only prefixes in the *access-list-name* argument with the same scope as the scope configured will be advertised. If no scope is configured, all scopes are advertised.

Examples The following example configures the router with the IPv6 address 2001:0DB8:3000:3000::42 to be advertised as the candidate RP, with a priority of 0:

```
Router(config)# ipv6 pim bsr candidate rp 2001:0DB8:3000:3000::42 priority 0
```

The following example configures the router with the IPv6 address 2001:0DB8:1:1:1 as the candidate RP for scope 6 for the group ranges specified in the access list named list1:

```
Router(config)# ipv6 pim bsr candidate rp 2001:0DB8:1:1:1 group-list list1 scope 6
```

Related Commands

Command	Description
ipv6 pim bsr candidate bsr	Configures a router as a candidate BSR.
ipv6 pim bsr border	Configures a border for all BSMs of any scope.

ipv6 pim dr-priority

To configure the designated router (DR) priority on a Protocol Independent Multicast (PIM) router, use the **ipv6 pim dr-priority** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ipv6 pim dr-priority *value*

no ipv6 pim dr-priority

Syntax Description

value	An integer value to represent DR priority. Value range is from 0 to 4294967294. The default value is 1.

Command Default

Default value is 1.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
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.
12.2(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 **ipv6 pim dr-priority** command configures the neighbor priority used for PIM DR election. The router with the highest DR priority on an interface becomes the PIM DR. If several routers have the same priority, then the router with the highest IPv6 address on the interface becomes the DR.

If a router does not include the DR priority option in its hello messages, then the router is considered to be the highest-priority router and becomes the DR. If several routers do not include the DR priority option in their hello messages, then the router with the highest IPv6 address becomes the DR.

Examples

The following example configures the router to use DR priority 3:

```
Router(config)# interface FastEthernet 1/0
Router(config-if)# ipv6 pim dr-priority 3
```

Related Commands

Command	Description
ipv6 pim hello-interval	Configures the frequency of PIM hello messages on an interface.

ipv6 pim hello-interval

To configure the frequency of Protocol Independent Multicast (PIM) hello messages on an interface, use the **ipv6 pim hello-interval** command in interface configuration mode. To return to the default interval, use the **no** form of this command.

ipv6 pim hello-interval *seconds*

no ipv6 pim hello-interval *seconds*

Syntax Description

seconds	Interval, in seconds, at which PIM hello messages are sent.

Command Default

Hello messages are sent at 30-second intervals with small random jitter.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
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.
12.2(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

Periodic hello messages are sent out at 30-second intervals with a small jitter. The **ipv6 pim hello-interval** command allows users to set a periodic interval.

Examples

The following example sets the PIM hello message interval to 45 seconds:

```
Router(config)# interface FastEthernet 1/0
Router(config-if)# ipv6 pim hello-interval 45
```

Related Commands

Command	Description
ipv6 mld query-interval	Configures the frequency at which the Cisco IOS software sends MLD host-query messages.

Command	Description
ipv6 pim dr-priority	Configures the DR priority on a PIM router.
show ipv6 pim neighbor	Displays the PIM neighbors discovered by the Cisco IOS software.

ipv6 pim join-prune-interval

To configure periodic join and prune announcement intervals for a specified interface, use the **ipv6 pim join-prune-interval** command in interface configuration mode. To return to the default value, use the **no** form of the command.

ipv6 pim join-prune-interval *seconds*

no ipv6 pim join-prune-interval *seconds*

Syntax Description

seconds	The join and prune announcement intervals, in number of seconds. The default value is 60 seconds.

Command Default

The default is 60 seconds.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.3(4)T	This command was 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(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

Periodic join and prune announcements are sent out at 60-second intervals. The **ipv6 pim join-prune-interval** command allows users to set a periodic interval.

Examples

The following example sets the join and prune announcement intervals to 75 seconds:

```
Router(config)# interface FastEthernet 1/0
Router(config-if)# ipv6 pim join-prune-interval 75
```

ipv6 pim neighbor-filter list

To filter Protocol Independent Multicast (PIM) neighbor messages from specific IPv6 addresses, use the **ipv6 pim neighbor-filter** command in the global configuration mode. To return to the router default, use the **no** form of this command.

ipv6 pim [**vrf** *vrf-name*] **neighbor-filter list** *access-list*

no ipv6 pim [**vrf** *vrf-name*] **neighbor-filter list** *access-list*

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
access-list	Name of an IPv6 access list that denies PIM hello packets from a source.

Command Default

PIM neighbor messages are not filtered.

Command Modes

Global configuration

Command History

Release	Modification
12.4(2)T	This command was introduced.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

The **ipv6 pim neighbor-filter list** command is used to prevent unauthorized routers on the LAN from becoming PIM neighbors. Hello messages from addresses specified in this command are ignored.

Examples

The following example causes PIM to ignore all hello messages from IPv6 address FE80::A8BB:CCFF:FE03:7200:

```
Router(config)# ipv6 pim neighbor-filter list nbr_filter_acl
Router(config)# ipv6 access-list nbr_filter_acl
Router(config-ipv6-acl)# deny ipv6 host FE80::A8BB:CCFF:FE03:7200 any
Router(config-ipv6-acl)# permit any any
```

ipv6 pim passive

To enable the Protocol Independent Multicast (PIM) passive feature on a specific interface, use the **ipv6 pim passive** command in interface configuration mode. To disable this feature, use the **no** form of this command.

ipv6 pim passive

no ipv6 pim passive

Syntax Description

This command has no arguments or keywords.

Command Default

PIM passive mode is not enabled on the router.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.

Usage Guidelines

Use the **ipv6 pim passive** command to configure IPv6 PIM passive mode on an interface.

A PIM passive interface does not send or receive any PIM control messages. However, a PIM passive interface acts as designated router (DR) and designated forwarder (DF)-election winner, and it can accept and forward multicast data.

Examples

The following example configures IPv6 PIM passive mode on an interface:

```
Router(config)# interface gigabitethernet 1/0/0
Router(config-if)# ipv6 pim passive
```

Related Commands

Command	Description
ipv6 multicast pim-passive-enable	Enables the PIM passive feature on an IPv6 router.

ipv6 pim rp embedded

To enable embedded rendezvous point (RP) support in IPv6 Protocol Independent Multicast (PIM), use the **ipv6 pim rp-embedded** command in global configuration mode. To disable embedded RP support, use the **no** form of this command.

ipv6 pim [**vrf** *vrf-name*] **rp embedded**

no ipv6 pim [**vrf** *vrf-name*] **rp embedded**

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Default

Embedded RP support is enabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
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(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
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.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

Because embedded RP support is enabled by default, users will generally use the **no** form of this command to turn off embedded RP support.

The **ipv6 pim rp embedded** command applies only to the embedded RP group ranges ff7X::/16 and fffX::/16. When the router is enabled, it parses groups in the embedded RP group ranges ff7X::/16 and fffX::/16, and extracts the RP to be used from the group address.

Examples

The following example disables embedded RP support in IPv6 PIM:

```
no ipv6 pim rp embedded
```

ipv6 pim rp-address

To configure the address of a Protocol Independent Multicast (PIM) rendezvous point (RP) for a particular group range, use the **ipv6 pim rp-address** command in global configuration mode. To remove an RP address, use the **no** form of this command.

ipv6 pim [**vrf** *vrf-name*] **rp-address** *ipv6-address* [*group-access-list*] [**bidir**]

no ipv6 pim rp-address *ipv6-address* [*group-access-list*] [**bidir**]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
ipv6-address	The IPv6 address of a router to be a PIM RP. The *ipv6-address* argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
group-access-list	(Optional) Name of an access list that defines for which multicast groups the RP should be used. If the access list contains any group address ranges that overlap the assigned source-specific multicast (SSM) group address range (FF3x::/96), a warning message is displayed, and the overlapping ranges are ignored. If no access list is specified, the specified RP is used for all valid multicast non-SSM address ranges. To support embedded RP, the router configured as the RP must use a configured access list that permits the embedded RP group ranges derived from the embedded RP address. Note that the embedded RP group ranges need not include all the scopes (for example, 3 through 7).
bidir	(Optional) Indicates that the group range will be used for bidirectional shared-tree forwarding; otherwise, it will be used for sparse-mode forwarding. A single IPv6 address can be configured to be RP only for either bidirectional or sparse-mode group ranges. A single group-range list can be configured to operate either in bidirectional or sparse mode.

Command Default

No PIM RPs are preconfigured.
Embedded RP support is enabled by default when IPv6 PIM is enabled (where embedded RP support is provided).
Multicast groups operate in PIM sparse mode.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.

Release	Modification
12.0(26)S	Embedded RP support was added.
12.3(7)T	The **bidir** keyword was added to Cisco IOS Release 12.3(7)T.
12.2(25)S	The **bidir** keyword was added to Cisco IOS Release 12.2(25)S.
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.
12.2(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.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

When PIM is configured in sparse mode, you must choose one or more routers to operate as the RP. An RP is a single common root of a shared distribution tree and is statically configured on each router.

Where embedded RP support is available, only the RP needs to be statically configured as the RP for the embedded RP ranges. No additional configuration is needed on other IPv6 PIM routers. The other routers will discover the RP address from the IPv6 group address. If these routers want to select a static RP instead of the embedded RP, the specific embedded RP group range must be configured in the access list of the static RP.

The RP address is used by first-hop routers to send register packets on behalf of source multicast hosts. The RP address is also used by routers on behalf of multicast hosts that want to become members of a group. These routers send join and prune messages to the RP.

If the optional *group-access-list* argument is not specified, the RP is applied to the entire routable IPv6 multicast group range, excluding SSM, which ranges from FFX[3-f]::/8 to FF3X::/96. If the *group-access-list* argument is specified, the IPv6 address is the RP address for the group range specified in the *group-access-list* argument.

You can configure Cisco IOS software to use a single RP for more than one group. The conditions specified by the access list determine which groups the RP can be used for. If no access list is configured, the RP is used for all groups.

A PIM router can use multiple RPs, but only one per group.

Examples

The following example shows how to set the PIM RP address to 2001::10:10 for all multicast groups:

```
Router(config)# ipv6 pim rp-address 2001::10:10
```

The following example sets the PIM RP address to 2001::10:10 for the multicast group FF04::/64 only:

```
Router(config)# ipv6 access-list acc-grp-1
Router(config-ipv6-acl)# permit ipv6 any ff04::/64
Router(config)# ipv6 pim rp-address 2001::10:10 acc-grp-1
```

The following example shows how to configure a group access list that permits the embedded RP ranges derived from the IPv6 RP address 2001:0DB8:2::2:

```
Router(config)# ipv6 pim rp-address 2001:0DB8:2::2 embd-ranges
Router(config)# ipv6 access-list embd-ranges
Router(config-ipv6-acl)# permit ipv6 any ff73:240:2:2:2::/96
Router(config-ipv6-acl)# permit ipv6 any ff74:240:2:2:2::/96
Router(config-ipv6-acl)# permit ipv6 any ff75:240:2:2:2::/96
```

```
Router(config-ipv6-acl)# permit ipv6 any ff76:240:2:2:2::/96
Router(config-ipv6-acl)# permit ipv6 any ff77:240:2:2:2::/96
Router(config-ipv6-acl)# permit ipv6 any ff78:240:2:2:2::/96
```

The following example shows how to enable the address 100::1 as the bidirectional RP for the entries multicast range FF::/8:

```
ipv6 pim rp-address 100::1 bidir
```

In the following example, the IPv6 address 200::1 is enabled as the bidirectional RP for the ranges permitted by the access list named bidir-grps. The ranges permitted by this list are ff05::/16 and ff06::/16.

```
Router(config)# ipv6 access-list bidir-grps
Router(config-ipv6-acl)# permit ipv6 any ff05::/16
Router(config-ipv6-acl)# permit ipv6 any ff06::/16
Router(config-ipv6-acl)# exit
Router(config)# ipv6 pim rp-address 200::1 bidir-grps bidir
```

Related Commands

Command	Description
debug ipv6 pim df-election	Displays debug messages for PIM bidirectional DF-election message processing.
ipv6 access-list	Defines an IPv6 access list and places the router in IPv6 access list configuration mode.
show ipv6 pim df	Displays the DF -election state of each interface for each RP.
show ipv6 pim df winner	Displays the DF-election winner on each interface for each RP.

ipv6 pim spt-threshold infinity

To configure when a Protocol Independent Multicast (PIM) leaf router joins the shortest path tree (SPT) for the specified groups, use the **ipv6 pim spt-threshold infinity** command in global configuration mode. To restore the default value, use the **no** form of this command.

ipv6 pim [**vrf** *vrf-name*] **spt-threshold infinity** [**group-list** *access-list-name*]

no ipv6 pim spt-threshold infinity

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
group-list *access-list-name*	(Optional) Indicates to which groups the threshold applies. Must be a standard IPv6 access list name. If the value is omitted, the threshold applies to all groups.

Command Default

When this command is not used, the PIM leaf router joins the SPT immediately after the first packet arrives from a new source. Once the router has joined the SPT, configuring the **ipv6 pim spt-threshold infinity** command will not cause it to switch to the shared tree.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
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.
12.2(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.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

Using the **ipv6 pim spt-threshold infinity** command enables all sources for the specified groups to use the shared tree. The **group-list** keyword indicates to which groups the SPT threshold applies.

The *access-list-name* argument refers to an IPv6 access list. When the *access-list-name* argument is specified with a value of 0, or the **group-list** keyword is not used, the SPT threshold applies to all groups. The default setting (that is, when this command is not enabled) is to join the SPT immediately after the first packet arrives from a new source.

Examples

The following example configures a PIM last-hop router to stay on the shared tree and not switch to the SPT for the group range ff04::/64.:

```
Router(config)# ipv6 access-list acc-grp-1
Router(config-ipv6-acl)# permit ipv6 any FF04::/64
Router(config-ipv6-acl)# exit
Router(config)# ipv6 pim spt-threshold infinity group-list acc-grp-1
```

ipv6 policy route-map

To configure IPv6 policy-based routing (PBR) on an interface, use the **ipv6 policy route-map** command in interface configuration mode. To disable PBR on an interface, use the **no** form of this command.

ipv6 policy route-map *route-map-name*

no ipv6 policy route-map *route-map-name*

Syntax Description

route-map-name	Name of the route map to use for PBR. The name must match a *map-tag* value specified by a **route-map** command.

Command Default

Policy routing does not occur on the interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)S.
12.2(33)SXI4	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SXI4.
Cisco IOS XE Release 3.2S	This command was modified. It was integrated into Cisco IOS XE Release 3.2S.

Usage Guidelines

You could enable PBR if you want your packets to take a route other than the obvious shortest path.

The **ipv6 policy route-map** command identifies a route map to use for policy-based routing. The **route-map** commands each have a list of **match** and **set** commands associated with them. The **match** commands specify the match criteria—the conditions under which PBR is allowed for the interface. The **set** commands specify the set actions—the particular PBR actions to perform if the criteria enforced by the **match** commands are met. The **no ipv6 policy route-map** command deletes the pointer to the route map.

Policy-based routing can be performed on any match criteria that can be defined in an IPv6 access list.

Examples

In the following example, a route map named pbr-dest-1 is created and configured, specifying packet match criteria and desired policy-route action. Then, PBR is enabled on Ethernet interface 0/0:

```
ipv6 access-list match-dest-1
  permit ipv6 any 2001:1760::/32

route-map pbr-dest-1 permit 10
  match ipv6 address match-dest-1
  set interface Ethernet0/0
```

```
interface Ethernet0/0
  ipv6 policy-route-map pbr-dest-1
```

Related Commands

Command	Description
ipv6 local policy route-map	Identifies a route map to use for local IPv6 PBR.
match ipv6 address	Specifies an IPv6 access list to use to match packets for PBR for IPv6.
match length	Bases policy routing on the Level 3 length of a packet.
route-map (IP)	Define the conditions for redistributing routes from one routing protocol into another, or to enable policy routing.
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Indicates where to output packets that pass a match clause of a route map for policy routing.
set ipv6 default next-hop	Specifies an IPv6 default next hop to which matching packets will be forwarded.
set ipv6 next-hop	Indicates where to output IPv6 packets that pass a match clause of a route map for policy routing.
set ipv6 precedence	Sets the precedence value in the IPv6 packet header.

ipv6 port-map

To establish port-to-application mapping (PAM) for the system, use the **ipv6 port-map** command in global configuration mode. To delete user-defined PAM entries, use the **no** form of this command.

ipv6 port-map {*application* **port** *port-num* [**list** *acl-name*]}

no ipv6 port-map {*application* **port** *port-num* [**list** *acl-name*]}

Syntax Description

application	Specifies the predefined application that requires port mapping.
port *port-num*	Specifies a port number. The range is from 1 to 65535.
list *acl-name*	(Optional) Specifies the name of the IPv6 access list (ACL) associated with the port mapping.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
12.3(11)T	This command was introduced.

Usage Guidelines

The **ipv6 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.

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 feature requires the system-defined mapping information to function properly. System-defined mapping information cannot be deleted or changed; that is, you cannot map HTTP services to port 21 (FTP) or FTP services to port 80 (HTTP).

Table 32 lists the default system-defined services and applications in the PAM table.

Table 32 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 the system-defined entries for a specific host or subnet using the **list** keyword in the **ipv6 port-map** command.

User-Defined Port Mapping

Network applications that use non-standard ports require user-defined entries in the mapping table. Use the **ipv6 port-map** command to create default user-defined entries in the PAM table.

To map a range of port numbers with a service or application, you must create a separate entry for each port number.

Note If you try to map an application to a system-defined port, a message appears warning you of a mapping conflict.

Use the **no** form of the **ipv6 port-map** command to delete user-defined entries from the PAM table.

To overwrite an existing user-defined port mapping, use the **ipv6 port-map** command to associate another service or application with the specific port.

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** keyword for the **ipv6 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 user-defined port-mapping configuration map port 8080 to the HTTP application:

```
ipv6 port-map http port 8080
```

Host-specific port-mapping configuration maps port 2121 to the FTP application from a particular set of host. First, the user needs to create a permit IPv6 access list for the allowed host(s). In the following example, packets from the hosts in the 2001:0DB8:1:7 subset destined for port 2121 will be mapped to the FTP application:

```
Router(config)# ipv6 access-list ftp-host
Router(config-ipv6-acl)# permit 2001:0DB8:1:7::/64 any
```

The port-map configuration is then configured as follows:

```
Router(config)# ipv6 port-map ftp port 2121 list ftp-host
```

Related Commands

Command	Description
show ipv6 port-map	Displays IPv6 port-mapping information.

ipv6 prefix-list

To create an entry in an IPv6 prefix list, use the **ipv6 prefix-list** command in global configuration mode. To delete the entry, use the **no** form of this command.

ipv6 prefix-list *list-name* [**seq** *seq-number*] {**deny** *ipv6-prefix*/*prefix-length* | **permit** *ipv6-prefix*/*prefix-length* | **description** *text*} [**ge** *ge-value*] [**le** *le-value*]

no ipv6 prefix-list *list-name*

Syntax Description

list-name	Name of the prefix list. • Cannot be the same name as an existing access list. • Cannot be the name "detail" or "summary" because they are keywords in the **show ipv6 prefix-list** command.
seq *seq-number*	(Optional) Sequence number of the prefix list entry being configured.
deny	Denies networks that matches the condition.
permit	Permits networks that matches the condition.
ipv6-prefix	The IPv6 network assigned to the specified prefix list. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/prefix-length	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
description *text*	A description of the prefix list that can be up to 80 characters in length.
ge *ge-value*	(Optional) Specifies a prefix length greater than or equal to the *ipv6-prefix*/*prefix-length* arguments. It is the lowest value of a range of the *length* (the "from" portion of the length range).
le *le-value*	(Optional) Specifies a prefix length less than or equal to the *ipv6-prefix* /*prefix-length* arguments. It is the highest value of a range of the *length* (the "to" portion of the length range).

Command Default

No prefix list is created.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)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 Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Release	Modification
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
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 **ipv6 prefix-list** command is similar to the **ip prefix-list** command, except that it is IPv6-specific.

To suppress networks from being advertised in updates, use the **distribute-list out** command.

The sequence number of a prefix list entry determines the order of the entries in the list. The router compares network addresses to the prefix list entries. The router begins the comparison at the top of the prefix list, with the entry having the lowest sequence number.

If multiple entries of a prefix list match a prefix, the entry with the lowest sequence number is considered the real match. Once a match or deny occurs, the router does not go through the rest of the prefix list. For efficiency, you may want to put the most common permits or denies near the top of the list, using the *seq-number* argument.

The **show ipv6 prefix-list** command displays the sequence numbers of entries.

IPv6 prefix lists are used to specify certain prefixes or a range of prefixes that must be matched before a permit or deny statement can be applied. Two operand keywords can be used to designate a range of prefix lengths to be matched. A prefix length of less than, or equal to, a value is configured with the **le** keyword. A prefix length greater than, or equal to, a value is specified using the **ge** keyword. The **ge** and **le** keywords can be used to specify the range of the prefix length to be matched in more detail than the usual *ipv6-prefix*/*prefix-length* argument. For a candidate prefix to match against a prefix list entry three conditions can exist:

- the candidate prefix must match the specified prefix list and prefix length entry
- the value of the optional **le** keyword specifies the range of allowed prefix lengths from the *prefix-length* argument up to, and including, the value of the **le** keyword
- the value of the optional **ge** keyword specifies the range of allowed prefix lengths from the value of the **ge** keyword up to, and including, 128.

Note Note that the first condition must match before the other conditions take effect.

An exact match is assumed when the **ge** or **le** keywords are not specified. If only one keyword operand is specified then the condition for that keyword is applied, and the other condition is not applied. The *prefix-length* value must be less than the **ge** value. The **ge** value must be less than, or equal to, the **le** value. The **le** value must be less than or equal to 128.

Every IPv6 prefix list, including prefix lists that do not have any permit and deny condition statements, has an implicit deny any any statement as its last match condition.

Examples

The following example denies all routes with a prefix of ::/0.

```
Router(config)# ipv6 prefix-list abc deny ::/0
```

The following example permits the prefix 2002::/16:

```
Router(config)# ipv6 prefix-list abc permit 2002::/16
```

The following example shows how to specify a group of prefixes to accept any prefixes from prefix 5F00::/48 up to and including prefix 5F00::/64.

```
Router(config)# ipv6 prefix-list abc permit 5F00::/48 le 64
```

The following example denies prefix lengths greater than 64 bits in routes that have the prefix 2001:0DB8::/64.

```
Router(config)# ipv6 prefix-list abc permit 2001:0DB8::/64 le 128
```

The following example permits mask lengths from 32 to 64 bits in all address space.

```
Router(config)# ipv6 prefix-list abc permit ::/0 ge 32 le 64
```

The following example denies mask lengths greater than 32 bits in all address space.

```
Router(config)# ipv6 prefix-list abc deny ::/0 ge 32
```

The following example denies all routes with a prefix of 2002::/128.

```
Router(config)# ipv6 prefix-list abc deny 2002::/128
```

The following example permits all routes with a prefix of ::/0.

```
Router(config)# ipv6 prefix-list abc permit ::/0
```

Related Commands

Command	Description
clear ipv6 prefix-list	Resets the hit count of the IPv6 prefix list entries.
distribute-list out	Suppresses networks from being advertised in updates.
ipv6 prefix-list sequence-number	Enables the generation of sequence numbers for entries in an IPv6 prefix list.
match ipv6 address	Distributes IPv6 routes that have a prefix permitted by a prefix list.
show ipv6 prefix-list	Displays information about an IPv6 prefix list or IPv6 prefix list entries.

ipv6 prefix-list sequence-number

To enable the generation of sequence numbers for entries in an IPv6 prefix list, use the **ipv6 prefix-list sequence-number** command in global configuration mode. To disable the generation of sequence numbers, use the **no** form of this command.

ipv6 prefix-list sequence-number

no ipv6 prefix-list sequence-number

Syntax Description

This command has no arguments or keywords.

Command Default

Sequence numbers are automatically generated for entries in an IPv6 prefix list.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)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 Release 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.

Usage Guidelines

To suppress sequence numbers use the **no ipv6 prefix-list sequence-number** command. If you disable the generation of sequence numbers in an IPv6 prefix list, you must specify the sequence number for each entry using the *seq-number* argument of the **ipv6 prefix-list** command.

The **show ipv6 prefix-list** command displays the sequence numbers of entries.

Examples

The following example shows the automatic sequence number generation for entries in an IPv6 prefix list being disabled:

```
Router(config)# no ipv6 prefix-list sequence-number
```

Related Commands

Command	Description
ipv6 prefix-list	Creates an entry in an IPv6 prefix list.
show ipv6 prefix-list	Displays information about an IPv6 prefix list or IPv6 prefix list entries.

ipv6 redirects

To enable the sending of Internet Control Message Protocol (ICMP) IPv6 redirect messages if Cisco IOS software is forced to resend a packet through the same interface on which the packet was received, use the **ipv6 redirects** command in interface configuration mode. To disable the sending of redirect messages, use the **no** form of this command.

ipv6 redirects

no ipv6 redirects

Syntax Description

This command has no arguments or keywords.

Command Default

The sending of ICMP IPv6 redirect messages is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(4)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 Release 12.2(14)S.
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.
12.2(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 rate at which the router generates all IPv6 ICMP error messages can be limited by using the **ipv6 icmp error-interval** command.

Examples

The following example disables the sending of ICMP IPv6 redirect messages on Ethernet interface 0 and reenables the messages on Ethernet interface 1:

```
Router(config)# interface ethernet 0
Router(config-if)# no ipv6 redirects

Router(config)# interface ethernet 1
Router(config-if)# ipv6 redirects
```

To verify whether the sending of IPv6 redirect messages is enabled or disabled on an interface, enter the **show ipv6 interface** command:

```
Router# show ipv6 interface
```

```
Ethernet0 is up, line protocol is up
  IPv6 is stalled, link-local address is FE80::1
  Global unicast address(es):
    2000::1, subnet is 2000::/64
    3000::1, subnet is 3000::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are disabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses.

Ethernet1 is up, line protocol is up
  IPv6 is stalled, link-local address is FE80::2
  Global unicast address(es):
    2000::2, subnet is 2000::/64
    3000::3, subnet is 3000::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is disabled, number of DAD attempts: 0
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses.
```

Related Commands

Command	Description
ipv6 icmp error-interval	Configures the interval for IPv6 ICMP error messages.

ipv6 rip default-information

To originate a default IPv6 route into the Routing Information Protocol (RIP), use the **ipv6 rip default-information** command in interface configuration mode. To remove the default IPv6 RIP route, use the **no** form of this command.

ipv6 rip *name* **default-information** {**only** | **originate**} [**metric** *metric-value*]

no ipv6 rip *name* **default-information**

Syntax Description

name	Name of the IPv6 RIP routing process.
only	Advertises the IPv6 default route (::/0) only. Suppresses the advertisement of all other routes.
originate	Advertises the IPv6 default route (::/0). The advertisement of other routes is unaffected.
metric *metric-value*	(Optional) Associates a metric with the default route. The *metric-value* range is from 1 through 15.

Command Default

Metric value is 1.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)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 Release 12.2(14)S.
12.3(14)T	The **metric** keyword and *metric-value* argument 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.
12.2(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 **ipv6 rip default-information** command is similar to the **default-information originate** (RIP) command, except that it is IPv6-specific.

Originating a default IPv6 route into RIP also forces the advertisement of the route in router updates sent on the interface. The advertisement of the route occurs regardless of whether the route is present in the IPv6 routing table.

The **metric** *metric-value* keyword and argument allow more flexibility in topologies with multiple RIP routers on a LAN. For example, a user may want to configure one of many routers on a LAN as the preferred default router, so that all default route traffic will transit this router. This function can be achieved by configuring the preferred router to advertise a default route with a lower metric than the other routers on the network.

Note To avoid routing loops after the IPv6 default route (::/0) is originated into a specified RIP routing process, the routing process ignores all default route information received in subsequent IPv6 RIP update messages.

Examples

The following example originates a default IPv6 route into RIP on Ethernet interface 0/0 and advertises only the default route in router updates sent on the interface:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 rip cisco default-information only
```

The following example originates a default IPv6 route into RIP on Ethernet interface 0/0 and advertises the default route with all other routes in router updates sent on the interface:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 rip cisco default-information originate
```

Related Commands

Command	Description
show ipv6 rip	Displays information about current IPv6 RIP processes.

ipv6 rip enable

To enable an IPv6 Routing Information Protocol (RIP) routing process on an interface, use the **ipv6 rip enable** command in interface configuration mode. To disable an IPv6 RIP routing process on an interface, use the **no** form of this command.

ipv6 rip *name* **enable**

no ipv6 rip *name*

Syntax Description

name	Name of the IPv6 RIP routing process.

Command Default

An IPv6 RIP routing process is not defined.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)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 Release 12.2(14)S.
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.
12.2(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 **ipv6 rip enable** interface configuration command is used to enable IPv6 RIP explicitly on required interfaces. In IPv4, the **network** *network-number* router configuration command is used to implicitly specify the interfaces on which to run IPv4 RIP.

Examples

The following example enables the IPv6 RIP routing process named cisco on Ethernet interface 0/0:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 rip cisco enable
```

Related Commands

Command	Description
show ipv6 rip	Displays information about current IPv6 RIP processes.

ipv6 rip metric-offset

To set the IPv6 Routing Information Protocol (RIP) metric for an interface, use the **ipv6 rip metric-offset** command in interface configuration mode. To return the metric to its default value, use the **no** form of this command.

ipv6 rip *word* **metric-offset** *value*

no ipv6 rip *word* **metric-offset**

Syntax Description

word	Name of the IPv6 RIP routing process.
value	Value added to the metric of an IPv6 RIP route received in a report message. A number from 1 to 16.

Command Default

The default metric value is 1.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)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 Release 12.2(14)S.
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.
12.2(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

When an IPv6 RIP route is received, the interface metric value set by the **ipv6 rip metric-offset** command is added before the route is inserted into the routing table. Therefore, increasing the IPv6 RIP metric value of an interface increases the metric value of IPv6 RIP routes received over the interface.

Use the **ipv6 rip metric-offset** command to influence which routes are used, as you prefer. The IPv6 RIP metric is in hop count.

Examples

The following example configures a metric increment of 10 for the RIP routing process named cisco on Ethernet interface 0/0:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 rip cisco metric-offset 10
```

Related Commands

Command	Description
show ipv6 rip	Displays information about current IPv6 RIP processes.

ipv6 rip summary-address

To configure IPv6 Routing Information Protocol (RIP) to advertise summarized IPv6 addresses on an interface and to specify the IPv6 prefix that identifies the routes to be summarized, use the **ipv6 rip summary-address** command in interface configuration mode. To stop the advertising of the summarized IPv6 addresses, use the **no** form of this command.

ipv6 rip *word* **summary-address** *ipv6-prefix*/*prefix-length*

no ipv6 rip *word* **summary-address**

Syntax Description

word	Name of the IPv6 RIP routing process.
ipv6-prefix	Specifies an IPv6 network number as the summary address. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/prefix-length	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

Command Default

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)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 Release 12.2(14)S.
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.
12.2(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 **ipv6 rip summary-address** command is similar to the **ip summary-address rip** command, except that it is IPv6-specific.

Use the **ipv6 rip summary-address** command to force IPv6 RIP to advertise specific networks on specific interfaces (assuming that routes to those networks exist).

If the first bits of the prefix length for a route match the value specified for the *ipv6-prefix* argument, the prefix specified in the *ipv6-prefix* argument is advertised instead of the route. As a result, multiple routes can be replaced by a single route whose metric is the lowest metric of the multiple routes.

Examples

In the following example, the IPv6 address 2001:0DB8:0:1:260:3EFF:FE11:6770 that is assigned to Ethernet interface 0/0 with an IPv6 prefix length of 64 bits is summarized as IPv6 prefix 2001:0DB8::/35 for the IPv6 RIP routing process named cisco:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 address 2001:0DB8:0:1:260:3EFF:FE11:6770 /64
Router(config-if)# ipv6 rip cisco summary-address 2001:0DB8::/35
```

Note A route advertisement that is suppressed as a result of split horizon is not considered by RIP when RIP is deciding whether to advertise a summary route.

Related Commands

Command	Description
poison-reverse (IPv6 RIP)	Configures the poison reverse processing of IPv6 RIP router updates.
show ipv6 rip	Displays information about current IPv6 RIP processes.

ipv6 route

To establish static IPv6 routes, use the **ipv6 route** command in global configuration mode. To remove a previously configured static route, use the **no** form of this command.

ipv6 route [**vrf** *vrf-name*] *ipv6-prefix*/*prefix-length* {*ipv6-address* | *interface-type interface-number* [*ipv6-address*]} [**nexthop-vrf** [*vrf-name1* | **default**]] [*administrative-distance*] [*administrative-multicast-distance* | **unicast** | **multicast**] [*next-hop-address*] [**tag** *tag*] [**name** *name*]

no ipv6 route [**vrf** *vrf-name*] *ipv6-prefix*/*prefix-length* {*ipv6-address* | *interface-type interface-number* [*ipv6-address*]} [**nexthop-vrf** [*vrf-name1* | **default**]] [*administrative-distance*] [*administrative-multicast-distance* | **unicast** | **multicast**] [*next-hop-address*] [**tag** *tag*] [**name** *route-name*]

Syntax Description

ipv6-prefix	The IPv6 network that is the destination of the static route. Can also be a host name when static host routes are configured.
/prefix-length	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
vrf	(Optional) Specifies all virtual private network (VPN) routing/forwarding instance (VRF) tables or a specific VRF table for IPv4 or IPv6 address.
vrf-name	(Optional) Names a specific VRF table for an IPv4 or IPv6 address.
ipv6-address	The IPv6 address of the next hop that can be used to reach the specified network. The IPv6 address of the next hop need not be directly connected; recursion is done to find the IPv6 address of the directly connected next hop. When an interface type and interface number are specified, you can optionally specify the IPv6 address of the next hop to which packets are output. **Note** You must specify an interface type and an interface number when using a link-local address as the next hop (the link-local next hop must also be an adjacent router). This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
interface-type	Interface type. For more information about supported interface types, use the question mark (?) online help function. You can use the *interface-type* argument to direct static routes out point-to-point interfaces (such as serial or tunnel interfaces) and broadcast interfaces (such as Ethernet interfaces). When using the *interface-type* argument with point-to-point interfaces, there is no need to specify the IPv6 address of the next hop. When using the *interface-type* argument with broadcast interfaces, you should always specify the IPv6 address of the next hop or ensure that the specified prefix is assigned to the link. A link-local address should be specified as the next hop for broadcast interfaces.

interface-number	Interface number. For more information about the numbering syntax for supported interface types, use the question mark (?) online help function.
nexthop-vrf	(Optional) Indicator that the next hop is a VRF.
vrf-name1	(Optional) Name of the next-hop VRF.
default	(Optional) Indicator that the next hop is the default.
administrative-distance	(Optional) An administrative distance. The default value is 1, which gives static routes precedence over any other type of route except connected routes.
administrative-multicast-distance	(Optional) The distance used when selecting this route for multicast Reverse Path Forwarding (RPF).
unicast	(Optional) Specifies a route that must not be used in multicast RPF selection.
multicast	(Optional) Specifies a route that must not be populated in the unicast Routing Information Base (RIB).
next-hop-address	(Optional) Address of the next hop that can be used to reach the specified network.
tag *tag*	(Optional) Tag value that can be used as a "match" value for controlling redistribution via route maps.
name *route-name*	(Optional) Specifies a name for the route.

Command Default

No static routes are established.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(4)T	The optional *ipv6-address* argument was added.
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 Release 12.2(14)S.
12.0(26)S	The optional **unicast** and **multicast** keywords and *administrative-multicast-distance* argument were added.
12.3(4)T	The optional **unicast** and **multicast** keywords and *administrative-multicast-distance* argument were added.
12.2(25)S	The optional **unicast** and **multicast** keywords and *administrative-multicast-distance* argument 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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	The optional **vrf** and **nexthop-vrf** keywords, and *vrf-name* and *next-hop-address* arguments were added.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 series routers.
15.0	The **name** *name* keyword and argument were added.

Usage Guidelines

Use the **ipv6 route** command to implement static multicast routes in IPv6. For a static multicast route, the IPv6 address of the next-hop router must be provided. The *administrative-multicast-distance* argument determines the distance that will be used when selecting this route for RPF. When the **unicast** keyword is used, this route will not be used in multicast RPF selection.

When the **ipv6 route** command is used with the **multicast** keyword, the route will not be populated in the unicast RIB. When the optional *administrative-multicast-distance* argument is not specified, the multicast RPF administrative distance defaults to the same value as that determined by the *administrative-distance* argument.

Examples

The following example shows a static route that applies to unicast routing only:

```
ipv6 route 2001::/64 5::5 100 unicast
```

The following example shows a static route used only for multicast RPF selection:

```
ipv6 route 2001::/64 7::7 100 multicast
```

The following example shows a static route used for both unicast routing and multicast RPF selection:

```
ipv6 route 2001::/64 6::6 100
```

The following example shows a static route used for both unicast routing and multicast RPF selection, but with different administrative distances:

```
ipv6 route 10::/64 7::7 100 200
```

The following example configures a static route for use in VPN for IPv6:

```
ipv6 route vrf red 4004::/64 pos 1/0
```

The following example configures a static default route within a VRF. Use of the **global** keyword in this static route provides access to the Internet:

```
ipv6 route vrf red ::0/0 7007::1 global
```

Related Commands

Command	Description
show ipv6 route	Displays the current contents of the IPv6 routing table.
show ipv6 route summary	Displays the current contents of the IPv6 routing table in summary format.
show ipv6 rpf	Displays RPF information for a given unicast host address and prefix.

ipv6 route static bfd

To specify static route Bidirectional Forwarding Detection for IPv6 (BFDv6) neighbors, use the **ipv6 route static bfd** command in global configuration mode. To remove a static route BFD neighbor, use the **no** form of this command.

ipv6 route static bfd [**vrf** *vrf-name*] *interface-type interface-number ipv6-address* [**unassociated**]

no ipv6 route static bfd

Syntax Description

vrf *vrf-name*	(Optional) Name of the virtual routing and forwarding (VRF) instance by which static routes should be specified.
interface-type interface-number	Interface type and number.
ipv6-address	IPv6 address of the neighbor.
unassociated	(Optional) Moves a static BFD neighbor from associated mode to unassociated mode.

Command Default

No static BFDv6 neighbors are specified.

Command Modes

Global configuration (config#)

Command History

Release	Modification
Cisco IOS XE Release 2.1.0	This command was introduced.
15.1(2)T	This command was modified. It was integrated into Cisco IOS Release 15.1(2)T.

Usage Guidelines

Use the **ipv6 route static bfd** command to specify static route neighbors. All of the static routes that have the same interface and gateway specified in the configuration share the same BFDv6 session for reachability notification. BFDv6 requires that BFDv6 sessions are initiated on both endpoint routers. Therefore, this command must be configured on each endpoint router. An IPv6 static BFDv6 neighbor must be fully specified (with the interface and the neighbor address) and must be directly attached.

All static routes that specify the same values for **vrf** *vrf-name*, *interface-type interface-number*, and *ipv6-address* will automatically use BFDv6 to determine gateway reachability and take advantage of fast failure detection.

Examples

The following example creates a neighbor on Ethernet 0/0 with an address of 2001::1:

```
Router(global)# ipv6 route static bfd ethernet 0/0 2001::1
```

The following example converts the neighbor to unassociated mode:

```
Router(global)# ipv6 route static bfd ethernet 0/0 2001::1 unassociated
```

Related Commands

Command	Description
show ipv6 static	Displays the current contents of the IPv6 routing table.

ipv6 route static resolve default

To allow a recursive IPv6 static route to resolve using the default IPv6 static route, use the **ipv6 route static resolve default** command in global configuration mode. To remove this function, use the **no** form of this command.

ipv6 route static resolve default

no ipv6 route static resolve default

Syntax Description

This command has no arguments or keywords.

Command Default

Recursive IPv6 static routes do not resolve via the default route.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)XNE	This command was introduced.

Usage Guidelines

By default, a recursive IPv6 static route will not resolve using the default route (::/0). The **ipv6 route static resolve default** command restores legacy behavior and allows resolution using the default route.

Examples

The following example enables an IPv6 recursive static route to be resolved using a IPv6 static default route:

```
Router(config)# ipv6 route static resolve default
```

ipv6 router eigrp

To place the router in router configuration mode, create an Enhanced Interior Gateway Routing Protocol (EIGRP) routing process in IPv6, and configure this process, use the **ipv6 router eigrp** command in global configuration mode. To shut down a routing process, use the **no** form of this command.

ipv6 router eigrp *as-number* [**eigrp event-log-size** *event-log-size*]

no ipv6 router eigrp *as-number*

Syntax Description

as-number	Autonomous system number.
eigrp event-log-size *event-log-size*	(Optional) Memory allocation value of the EIGRP event. The *event-log-size* value is the memory allocation, in bytes, calculated dynamically based on available memory. The *event-log-size* value is between 0 and the dynamically calculated number.

Command Default

This command is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SRB	The **eigrp event-log-size** keyword and *event-log-size* argument were 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 integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

Use the **ipv6 router eigrp** command in global configuration mode to place the router in router configuration mode and create a routing process. Once in router configuration mode, you can configure the EIGRP for IPv6 routing process using the **ipv6 router eigrp** command.

Examples

The following example places the router in router configuration mode and allows you to configure an EIGRP for IPv6 routing process:

```
Router(config)# ipv6 router eigrp 400

 eigrp router-id 10.13.14.15
 eigrp stub connected summary
 eigrp event-log-size 1000
 no shutdown
```

Related Commands

Command	Description
ipv6 eigrp	Enables EIGRP for IPv6 on a specified interface.
router eigrp	Configures the EIGRP process.

ipv6 router isis

To configure an Intermediate System-to-Intermediate System (IS-IS) routing process for IPv6 on an interface and to attach an area designator to the routing process, use the **ipv6 router isis** command in interface configuration mode. To disable IS-IS for IPv6, use the **no** form of the command.

ipv6 router isis *area-name*

no ipv6 router isis *area-name*

Syntax Description

area-name	Meaningful name for a routing process. If a name is not specified, a null name is assumed and the process is referenced with a null name. This name must be unique among all IP or Connectionless Network Service (CLNS) router processes for a given router. Required for multiarea IS-IS configuration. Each area in a multiarea configuration should have a nonnull area name to facilitate identification of the area. Optional for conventional IS-IS configuration.

Command Default

No routing processes are specified.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(8)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 Release 12.2(14)S.
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.
12.2(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 2.4	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

Before the IPv6 IS-IS routing process can be configured, IPv6 routing must be enabled using the **ipv6 unicast-routing** global configuration command, and an IPv6 address must be configured on an interface using either the **ipv6 enable** interface configuration command or the **ipv6 address** interface configuration command. The **ipv6 enable** command will automatically configure an IPv6 link-local address on the interface.

Examples

The following example specifies IS-IS as an IPv6 routing protocol for a process named Finance. The Finance process will run over the Fast Ethernet interface 0/1.

```
Router(config)# router isis Finance
Router(config-router)# net 49.0001.aaaa.aaaa.aaaa.00
Router(config-router)# exit
Router(config)# interface FastEthernet 0/1
Router(config-if)# ipv6 router isis Finance
```

Related Commands

Command	Description
ipv6 address link-local	Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface.
ipv6 enable	Enables an interface for IPv6 processing and automatically assigns an IPv6 link-local address on the interface.
ipv6 unicast-routing	Enables the forwarding of IPv6 unicast datagrams.
net	Configures an IS-IS NET for a CLNS routing process.
router isis	Enables the IPv4 IS-IS routing protocol.

ipv6 router nemo

To enable the network mobility (NEMO) routing process on the home agent and place the router in router configuration mode, use the **ipv6 router nemo** command in global configuration mode. To disable this function, use the **no** form of the command.

ipv6 router nemo

no ipv6 router nemo

Syntax Description

This command has no arguments or keywords.

Command Default

The NEMO routing process is not enabled on the home agent.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

This command enables the NEMO routing process on the home agent.

Examples

In the following example, NEMO is enabled on the home agent:

```
Router(config)# ipv6 router nemo
```

ipv6 router ospf

To enable Open Shortest Path First (OSPF) for IPv6 router configuration mode, use the **ipv6 router ospf** command in global configuration mode.

ipv6 router ospf *process-id*

Syntax Description

process-id	Internal identification. It is locally assigned and can be a positive integer from 1 to 65535. The number used here is the number assigned administratively when enabling the OSPF for IPv6 routing process.

Command Default

No OSPF for IPv6 routing process is defined.

Command Modes

Global configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
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.
12.2(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.
15.0(1)M	This command was modified. It was integrated into Cisco IOS Release 15.0(1)M.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.
15.1(2)T	This command was modified. Support for IPv6 was added to Cisco IOS Release 15.1(2)T.

Usage Guidelines

Use this command to enter the OSPF for IPv6 router configuration mode. From this mode, you can enter several commands to customize OSPF for IPv6.

Examples

The following example enables router OSPF for IPv6 configuration mode and identifies the process with the number 1:

```
ipv6 router ospf 1
```

ipv6 router rip

To configure an IPv6 Routing Information Protocol (RIP) routing process, use the **ipv6 router rip** command in global configuration mode. To remove a routing process, use the **no** form of this command.

ipv6 router rip *word*

no ipv6 router rip *word*

Syntax Description

word	A word that describes the routing process.

Command Default

No IPv6 RIP routing process is defined.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)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 Release 12.2(14)S.
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.
12.2(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 **ipv6 router rip** command is similar to the **router rip** command, except that it is IPv6-specific.

Use this command to enable an IPv6 RIP routing process. Configuring this command places the router in router configuration mode for the IPv6 RIP routing process. The router prompt changes to Router(config-rtr-rip)#.

Examples

The following example configures the IPv6 RIP routing process named cisco and places the router in router configuration mode for the IPv6 RIP routing process:

```
Router(config)# ipv6 router rip cisco
```

Related Commands

Command	Description
ipv6 rip enable	Enables an IPv6 RIP routing process on an interface.

ipv6 routing-enforcement-header loose

To provide backward compatibility with legacy IPv6 inspection, use the **ipv6 routing-enforcement-header loose** command in parameter map type inspect configuration mode. To disable this feature, use the **no** form of this command.

ipv6 routing-enforcement-header loose

no ipv6 routing-enforcement-header loose

Syntax Description

This command has no arguments or keywords.

Command Default

Backward compatibility is not provided.

Command Modes

parameter map type inspect configuration mode (config-profile)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **ipv6 routing-enforcement-header loose** command provides backward compatibility with legacy IPv6 inspection. Enabling this command ensures that the firewall will not drop IPv6 traffic with routing headers. The default firewall behavior is to drop all IPv6 traffic without a routing header.

Examples

The following example enables backward compatibility with legacy IPv6 inspection on an inspect type parameter map named v6-param-map:

```
Router(config)# parameter-map type inspect v6-param-map
Router (config-profile)# ipv6 routing-header-enforcement loose
```

Related Commands

Command	Description
parameter-map type inspect	Configures an inspect type parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action.

ipv6 snooping logging packet drop

To enable the logging of dropped packets by the IPv6 first-hop security feature, use the **ipv6 snooping logging packet drop** command in global configuration mode. To disable the logging of dropped packets by the IPv6 first-hop security feature, use the **no** form of this command.

ipv6 snooping logging packet drop

no ipv6 snooping logging packet drop

Syntax Description

This command has no arguments or keywords.

Command Default

Snooping security logging is not enabled.

Command Modes

Global configuration (config)#

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

Use the **ipv6 snooping logging packet drop** command to log packets that are dropped when they are received on an unauthorized port. For example, this command will log RA packets that are dropped because of the RA guard feature.

Related Commands

Command	Description
ipv6 neighbor binding logging	Enables the logging of binding table main events.

ipv6 source-route

To enable processing of the IPv6 type 0 routing header (the IPv6 source routing header), use the **ipv6 source-route** command in global configuration mode. To disable the processing of this IPv6 extension header, use the **no** form of this command.

ipv6 source-route

no ipv6 source-route

Syntax Description

This command has no arguments or keywords.

Command Default

The **no** version of the **ipv6 source-route** command is the default. When the router receives a packet with a type 0 routing header, the router drops the packet and sends an IPv6 Internet Control Message Protocol (ICMP) error message back to the source and logs an appropriate debug message.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(33)SRB1	This command was integrated into Cisco IOS Release 12.2(33)SRB1.
12.4(15)T	The default was changed to be the **no** version of the **ipv6 source-route** command. When the router receives a packet with a type 0 routing header, the router drops the packet and sends an IPv6 ICMP error message back to the source and logs an appropriate debug message.
12.2(33)SRC	Changes made to this command were integrated into Cisco IOS 12.2(33)SRC.
Cisco IOS XE Release 2.5	This command was updated. It was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

The default was changed to be the **no** version of the **ipv6 source-route** command, which means this functionality is not enabled. Before this change, this functionality was enabled automatically. User who had configured the **no ipv6 source-route** command before the default was changed will continue to see this configuration in their **show config** command output, even though the **no** version of the command is the default.

The **no ipv6 source-route** command (which is the default) prevents hosts from performing source routing using your routers. When the **no ipv6 source-route** command is configured and the router receives a packet with a type0 source routing header, the router drops the packet and sends an IPv6 ICMP error message back to the source and logs an appropriate debug message.

In IPv6, source routing is performed only by the destination of the packet. Therefore, in order to stop source routing from occurring inside your network, you need to configure an IPv6 access control list (ACL) that includes the following rule:

```
deny ipv6 any any routing
```

The rate at which the router generates all IPv6 ICMP error messages can be limited by using the **ipv6 icmp error-interval** command.

Examples

The following example disables the processing of IPv6 type 0 routing headers:

```
no ipv6 source-route
```

Related Commands

Command	Description
deny (IPv6)	Sets deny conditions for an IPv6 access list.
ipv6 icmp error-interval	Configures the interval for IPv6 ICMP error messages.

ipv6 spd mode

To configure an IPv6 Selective Packet Discard (SPD) mode, use the **ipv6 spd mode** command in global configuration mode. To remove the IPv6 SPD mode, use the **no** form of this command.

ipv6 spd mode {**aggressive | tos protocol ospf**}

no ipv6 spd mode {**aggressive | tos protocol ospf**}

Syntax Description

aggressive	Aggressive drop mode discards incorrectly formatted packets when the IPv6 SPD is in random drop state.
tos protocol ospf	OSPF mode allows OSPF packets to be handled with SPD priority.

Command Default

No IPv6 SPD mode is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T.

Usage Guidelines

The default setting for the IPv6 SPD mode is none, but you may want to use the **ipv6 spd mode** command to configure a mode to be used when a certain SPD state is reached.

The **aggressive** keyword enables aggressive drop mode, which drops deformed packets when IPv6 SPD is in random drop state. The **ospf** keyword enables OSPF mode, in which OSPF packets are handled with SPD priority.

The size of the process input queue governs the SPD state: normal (no drop), random drop, or max. When the process input queue is less than the SPD minimum threshold, SPD takes no action and enters normal state. In the normal state, no packets are dropped. When the input queue reaches the maximum threshold, SPD enters max state, in which normal priority packets are discarded. If the input queue is between the minimum and maximum thresholds, SPD enters the random drop state, in which normal packets may be dropped.

Examples

The following example shows how to enable the router to drop deformed packets when the router is in the random drop state:

```
Router(config)# ipv6 spf mode aggressive
```

Related Commands

Command	Description
ipv6 spd queue max-threshold	Configures the maximum number of packets in the IPv6 SPD process input queue.
ipv6 spd queue min-threshold	Configures the minimum number of packets in the IPv6 SPD process input queue.
show ipv6 spd	Displays the IPv6 SPD configuration.

ipv6 spd queue max-threshold

To configure the maximum number of packets in the IPv6 Selective Packet Discard (SPD) process input queue, use the **ipv6 spd queue max-threshold** command in global configuration mode. To return to the default value, use the **no** form of this command.

ipv6 spd queue max-threshold *value*

no ipv6 spd queue max-threshold

Syntax Description

value	Number of packets. The range is from 0 through 65535.

Command Default

No SPD queue maximum threshold value is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.
15.1(3)T	This command was modified. The *value* argument range was changed from 4096 through 65535 to 0 through 65535.

Usage Guidelines

Use the **ipv6 spd queue max-threshold** command to configure the SPD queue maximum threshold value.

The size of the process input queue governs the SPD state: normal (no drop), random drop, or max. When the process input queue is less than the SPD minimum threshold, SPD takes no action and enters normal state. In the normal state, no packets are dropped. When the input queue reaches the maximum threshold, SPD enters max state, in which normal priority packets are discarded. If the input queue is between the minimum and maximum thresholds, SPD enters the random drop state, in which normal packets may be dropped.

Examples

The following example shows how to set the maximum threshold value of the queue to 60,000:

```
Router(config)# ipv6 spd queue max-threshold 60000
```

Related Commands

Command	Description
ipv6 spd queue min-threshold	Configures the minimum number of packets in the IPv6 SPD process input queue.
show ipv6 spd	Displays the IPv6 SPD configuration.

ipv6 spd queue min-threshold

To configure the minimum number of packets in the IPv6 Selective Packet Discard (SPD) process input queue, use the **ipv6 spd queue min-threshold** command in global configuration mode. To return to the default value, use the **no** form of this command.

ipv6 spd queue min-threshold *value*

no ipv6 spd queue min-threshold

Syntax Description

value	Number of packets. The range is from 0 through 65535.

Command Default

No SPD queue minimum threshold is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T.

Usage Guidelines

Use the **ipv6 spd queue min-threshold** command to configure the SPD queue minimum threshold, which determines IPv6 state transition from normal to random drop state. The minimum threshold value must be lower than the maximum threshold setting.

The size of the process input queue governs the SPD state: normal (no drop), random drop, or max. When the process input queue is less than the SPD minimum threshold, SPD takes no action and enters normal state. In the normal state, no packets are dropped. When the input queue reaches the maximum threshold, SPD enters max state, in which normal priority packets are discarded. If the input queue is between the minimum and maximum thresholds, SPD enters the random drop state, in which normal packets may be dropped.

Examples

The following example shows how to set the IPv6 SPD minimum threshold to 4094 packets:

```
Router(config)# ipv6 spd queue min-threshold 4094
```

Related Commands

Command	Description
ipv6 spd queue max-threshold	Configures the maximum number of packets in the IPv6 SPD process input queue.
show ipv6 spd	Displays the IPv6 SPD configuration.

ipv6 split-horizon eigrp

To enable Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 split horizon, use the **ipv6 split-horizon eigrp** command in interface configuration mode. To disable split horizon, use the **no** form of this command.

ipv6 split-horizon eigrp *as-number*

no ipv6 split-horizon eigrp *as-number*

Syntax Description

as-number	Autonomous system number.

Command Default

EIGRP for IPv6 split horizon is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(6)T	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.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

For networks that include links over X.25 packet-switched networks (PSNs), you can use the **neighbor** command in router configuration mode to disable the split horizon feature. Or, you can specify the **no ipv6 split-horizon eigrp** command in your configuration. However, if you do disable the split horizon feature, you must similarly disable split horizon for all routers and access servers in any relevant multicast groups on that network.

Note In general, we recommend that you not change the default state of split horizon unless you are certain that your application requires the change in order to advertise routes properly. Remember that if split horizon is disabled on a serial interface and that interface is attached to a packet-switched network, you must disable split horizon for all routers and access servers in any relevant multicast groups on that network.

Examples

The following example disables split horizon on a serial link connected to an X.25 network:

```
interface serial 0
 encapsulation x25
 no ipv6 split-horizon eigrp 101
```

Related Commands

Command	Description
neighbor (EIGRP)	Defines a neighboring router with which to exchange routing information on a router that is running EIGRP.

ipv6 summary-address eigrp

To configure a summary aggregate address for a specified interface, use the **ipv6 summary-address eigrp** command in interface configuration mode. To disable a configuration, use the **no** form of this command.

ipv6 summary-address eigrp *as-number ipv6-address* [*admin-distance*]

no ipv6 summary-address eigrp *as-number ipv6-address* [*admin-distance*]

Syntax Description

as-number	Autonomous system number.
ipv6-address	Summary IPv6 address to apply to an interface.
admin-distance	(Optional) Administrative distance. A value from 0 through 255. The default value is 90.

Command Default

An administrative distance of 5 is applied to Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 summary routes.
EIGRP for IPv6 automatically summarizes to the network level, even for a single host route.
No summary addresses are predefined.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(6)T	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.

Usage Guidelines

The **ipv6 summary-address eigrp** command is used to configure interface-level address summarization. EIGRP for IPv6 summary routes are given an administrative distance value of 5. The administrative distance metric is used to advertise a summary address without installing it in the routing table.

Examples

The following example provides a summary aggregate address for EIGRP for IPv6 for AS 1:

```
ipv6 summary-address eigrp 1 2001:0DB8:0:1::/64
```

ipv6 tacacs source-interface

To specify an interface to use for the source address in TACACS packets, use the **ipv6 tacacs source-interface** command in global configuration mode. To remove the specified interface from the configuration, use the **no** form of this command.

ipv6 tacacs source-interface *interface*

no ipv6 tacacs source-interface *interface*

Syntax Description

interface	Interface to be used for the source address in TACACS packets.

Command Default

No interface is specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines

The **ipv6 tacacs source-interface** command specifies an interface to use for the source address in TACACS packets.

Examples

The following example shows how to configure the Gigabit Ethernet interface to be used as the source address in TACACS packets:

```
Router(config)# ipv6 tacacs source-interface GigabitEthernet 0/0/0
```

Related Commands

Command	Description
tacacs server	Configures the TACACS+ server for IPv6 or IPv4 and enters TACACS+ server configuration mode.

ipv6 traffic interface-statistics

To collect IPv6 forwarding statistics for all interfaces, use the **ipv6 traffic interface-statistics** command in global configuration mode. To ensure that IPv6 forwarding statistics are not collected for any interface, use the **no** form of this command.

ipv6 traffic interface-statistics [**unclearable**]

no ipv6 traffic interface-statistics [**unclearable**]

Syntax Description

unclearable	(Optional) IPv6 forwarding statistics are kept for all interfaces, but it is not possible to clear the statistics on any interface.

Command Default

IPv6 forwarding statistics are collected for all interfaces.

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

Using the optional **unclearable** keyword halves the per-interface statistics storage requirements.

Examples

The following example does not allow statistics to be cleared on any interface:

```
ipv6 traffic interface-statistics unclearable
```

ipv6 traffic-filter

To filter incoming or outgoing IPv6 traffic on an interface, use the **ipv6 traffic-filter** command in interface configuration mode. To disable the filtering of IPv6 traffic on an interface, use the **no** form of this command.

ipv6 traffic-filter *access-list-name* {**in** | **out**}

no ipv6 traffic-filter *access-list-name*

Syntax Description

access-list-name	Specifies an IPv6 access name.
in	Specifies incoming IPv6 traffic.
out	Specifies outgoing IPv6 traffic.

Command Default

Filtering of IPv6 traffic on an interface is not configured.

Command Modes

Interface configuration (config-if)
Policy-map configuration (config-pmap)

Command History

Release	Modification
12.2(2)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 Release 12.2(14)S.
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.
12.2(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 introduced on Cisco ASR 1000 series routers.
12.2(33)SXI4	The **out** keyword and therefore filtering of outgoing traffic is not supported in IPv6 port-based access list (PACL) configuration.
12.2(54)SG	This command was modified. Support for Cisco IOS Release 12.2(54)SG was added.
12.2(50)SY	This command was modified. The **out** keyword is not supported.

Examples

The following example filters inbound IPv6 traffic on Ethernet interface 0/0 as defined by the access list named cisco:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 traffic-filter cisco in
```

Related Commands

Command	Description
ipv6 access-list	Defines an IPv6 access list and sets deny or permit conditions for the defined access list.
show ipv6 access-list	Displays the contents of all current IPv6 access lists.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 unicast-routing

To enable the forwarding of IPv6 unicast datagrams, use the **ipv6 unicast-routing** command in global configuration mode. To disable the forwarding of IPv6 unicast datagrams, use the **no** form of this command.

ipv6 unicast-routing

no ipv6 unicast-routing

Syntax Description

This command has no arguments or keywords.

Command Default

IPv6 unicast routing is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)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 Release 12.2(14)S.
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.
12.2(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 introduced on Cisco ASR 1000 series routers.

Usage Guidelines

Configuring the **no ipv6 unicast-routing** command removes all IPv6 routing protocol entries from the IPv6 routing table.

Examples

The following example enables the forwarding of IPv6 unicast datagrams:

```
Router(config)# ipv6 unicast-routing
```

Related Commands

Command	Description
ipv6 address link-local	Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface.
ipv6 address eui-64	Configures an IPv6 address and enables IPv6 processing on an interface using an EUI-64 interface ID in the low-order 64 bits of the address.

Command	Description
ipv6 enable	Enables IPv6 processing on an interface that has not been configured with an explicit IPv6 address.
ipv6 unnumbered	Enables IPv6 processing on an interface without assigning an explicit IPv6 address to the interface.
show ipv6 route	Displays the current contents of the IPv6 routing table.

ipv6 unnumbered

To enable IPv6 processing on an interface without assigning an explicit IPv6 address to the interface, use the **ipv6 unnumbered** command in interface configuration mode. To disable IPv6 on an unnumbered interface, use the **no** form of this command.

ipv6 unnumbered *interface-type interface-number*

no ipv6 unnumbered

Syntax Description

interface-type	The interface type of the source address that the unnumbered interface uses in the IPv6 packets that it originates. The source address cannot be another unnumbered interface.
interface-number	The interface number of the source address that the unnumbered interface uses in the IPv6 packets that it originates.

Command Default

This command is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)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 Release 12.2(14)S.
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.
12.2(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

IPv6 packets that are originated from an unnumbered interface use the global IPv6 address of the interface specified in the **ipv6 unnumbered** command as the source address for the packets. The **ipv6 unnumbered** *interface* command is used as a hint when doing source address selection; that is, when trying to determine the source address of an outgoing packet.

Note Serial interfaces using High-Level Data Link Control (HDLC), PPP, Link Access Procedure, Balanced (LAPB), Frame Relay encapsulations, and tunnel interfaces can be unnumbered. You cannot use this interface configuration command with X.25 or Switched Multimegabit Data Service (SMDS) interfaces.

Examples

The following example configures serial interface 0/1as unnumbered. IPv6 packets that are sent on serial interface 0/1 use the IPv6 address of Ethernet 0/0 as their source address:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 address 3FFE:C00:0:1:260:3EFF:FE11:6770

Router(config)# interface serial 0/1
Router(config-if)# ipv6 unnumbered ethernet 0/0
```

Related Commands

Command	Description
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 unreachables

To enable the generation of Internet Control Message Protocol for IPv6 (ICMPv6) unreachable messages for any packets arriving on a specified interface, use the **ipv6 unreachables** command in interface configuration mode. To prevent the generation of unreachable messages, use the **no** form of this command.

ipv6 unreachables

no ipv6 unreachables

Syntax Description

This command has no arguments or keywords.

Command Default

ICMPv6 unreachable messages can be generated for any packets arriving on that interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(2)T	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.

Usage Guidelines

If the Cisco IOS software receives a nonbroadcast packet destined for itself that uses a protocol it does not recognize, it sends an ICMPv6 unreachable message to the source.

If the software receives a datagram that it cannot deliver to its ultimate destination because it knows of no route to the destination address, it replies to the originator of that datagram with an ICMP host unreachable message.

Examples

The following example enables the generation of ICMPv6 unreachable messages, as appropriate, on an interface:

```
interface ethernet 0
 ipv6 unreachables
```

ipv6 verify unicast reverse-path

To enable Unicast Reverse Path Forwarding (Unicast RPF) for IPv6, use the **ipv6 verify unicast reverse-path** command in interface configuration mode. To disable Unicast RPF, use the **no** form of this command.

ipv6 verify unicast reverse-path [**access-list** *name*]

no ipv6 verify unicast reverse-path [**access-list** *name*]

Syntax Description

access-list *name*	(Optional) Specifies the name of the access list. **Note** This keyword and argument are not supported on the Cisco 12000 series Internet router.

Command Default

Unicast RPF is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S and introduced on the 10G Engine 5 SPA Interface Processor in the Cisco 12000 series Internet router.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

The **ipv6 verify unicast reverse-path** command is used to enable Unicast RPF for IPv6 in strict checking mode. The Unicast RPF for IPv6 feature requires that Cisco Express Forwarding for IPv6 is enabled on the router.

Note Beginning in Cisco IOS Release 12.0(31)S, the Cisco 12000 series Internet router supports both the **ipv6 verify unicast reverse-path** and **ipv6 verify unicast source reachable-via rx** commands to enable Unicast RPF to be compatible with the Cisco IOS Release 12.3T and 12.2S software trains.

Use the **ipv6 verify unicast reverse-path** 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 denial-of-service (DoS) attacks based on source IP address spoofing.

When Unicast RPF is enabled on an interface, the router examines all packets received on that interface. The router checks to make sure that the source IPv6 address appears in the routing table and that it is reachable by a path through the interface on which the packet was received. Unicast RPF is an input feature and is applied only on the input interface of a router at the upstream end of a connection.

The Unicast RPF feature performs a reverse lookup in the CEF table to check if any packet received at a router interface has arrived on a path identified as a best return path 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, 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 RPF 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 RPF command. Log information can be used to gather information about the attack, such as source address, time, and so on.

Note When you configure Unicast RPF for IPv6 on the Cisco 12000 series Internet router, the most recently configured checking mode is not automatically applied to all interfaces as on other platforms. You must enable Unicast RPF for IPv6 separately on each interface.

When you configure a SPA on the Cisco 12000 series Internet router, the interface address is in the format *slot/subslot/port*.

The optional **access-list** keyword for the **ipv6 verify unicast reverse-path** command is not supported on the Cisco 12000 series Internet router. For information about how Unicast RPF can be used with ACLs on other platforms to mitigate the transmission of invalid IPv4 addresses (perform egress filtering) and to prevent (deny) the reception of invalid IPv4 addresses (perform ingress filtering), refer to the "Configuring Unicast Reverse Path Forwarding" chapter in the "Other Security Features" section of the *Cisco IOS Security Configuration Guide*.

Note When using 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).

Do not use Unicast RPF on core-facing interfaces that are internal to the network. Internal interfaces are likely to have routing asymmetry, meaning that there are multiple routes to the source of a packet. Apply Unicast RPF only where there is natural or configured symmetry.

For example, routers at the edge of the network of an Internet service provider (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. Hence, it is not recommended that you apply Unicast RPF where there is a chance of asymmetric routing. It is simplest to place Unicast RPF only at the edge of a network or, for an ISP, at the customer edge of the network.

Examples

Unicast Reverse Path Forwarding on a Serial Interface

The following example shows how to enable the Unicast RPF feature on a serial interface:

```
interface serial 5/0/0
  ipv6 verify unicast reverse-path
```

Unicast Reverse Path Forwarding on a Cisco 12000 Series Internet Router

The following example shows how to enable Unicast RPF for IPv6 with strict checking on a 10G SIP Gigabit Ethernet interface 2/1/2:

```
Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# interface gigabitEthernet 2/1/2

Router(config-if)# ipv6 verify unicast reverse-path
Router(config-if)# exit
```

Unicast Reverse Path Forwarding on a Single-Homed ISP

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 209.165.202.128/28 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.

```
interface Serial 5/0/0
description Connection to Upstream ISP
ipv6 address FE80::260:3EFF:FE11:6770/64
no ipv6 redirects
ipv6 verify unicast reverse-path abc
!
ipv6 access-list abc
permit ipv6 host 2::1 any
deny ipv6 FEC0::/10 any
  ipv6 access-group abc in
  ipv6 access-group jkl out
!
access-list abc permit ip FE80::260:3EFF:FE11:6770/64 2001:0DB8:0000:0001::0001any
access-list abc deny ipv6 any any log
access-list jkl deny ipv6 host 2001:0DB8:0000:0001::0001 any log
access-list jkl deny ipv6 2001:0DB8:0000:0001:FFFF:1234::5.255.255.255 any log
access-list jkl deny ipv6 2002:0EF8:002001:0DB8:0000:0001:FFFF:1234::5172.16.0.0
0.15.255.255 any log
access-list jkl deny ipv6 2001:0CB8:0000:0001:FFFF:1234::5 0.0.255.255 any log
access-list jkl deny ipv6 2003:0DB8:0000:0001:FFFF:1234::5 0.0.0.31 any log
access-list jkl permit ipv6
```

ACL Logging with Unicast RPF

The following example demonstrates the use of ACLs and logging with Unicast RPF. In this example, extended ACL abc provides entries that deny or permit network traffic for specific address ranges. Unicast RPF is configured on interface Ethernet 0/0 to check packets arriving at that interface.

For example, packets with a source address of 8765:4321::1 arriving at Ethernet interface 0 are dropped because of the deny statement in ACL “abc.” 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 1234:5678::1 arriving at Ethernet interface 0/0 are forwarded because of the permit statement in ACL abc. ACL information about dropped or suppressed packets is logged (the logging option is turned on for the ACL entry) to the log server.

```
interface ethernet 0/0
ipv6 address FE80::260:3EFF:FE11:6770/64 link-local
ipv6 verify unicast reverse-path abc
!
ipv6 access-list abc
```

```
permit ipv6 1234:5678::/64 any log-input
deny ipv6 8765:4321::/64 any log-input
```

Related Commands

Command	Description
ip cef	Enables Cisco Express Forwarding on the route processor card.
ip verify unicast reverse-path	Enables Unicast RPF for IPv4 traffic.
ipv6 cef	Enables Cisco Express Forwarding for IPv6 interfaces.

ipv6 verify unicast source reachable-via

To verify that a source address exists in the FIB table and enable Unicast Reverse Path Forwarding (Unicast RPF), use the **ipv6 verify unicast source reachable-via** command in interface configuration mode. To disable URPF, use the **no** form of this command.

ipv6 verify unicast source reachable-via {**rx** | **any**} [**allow-default**] [**allow-self-ping**] [*access-list-name*]

no ipv6 verify unicast

Syntax Description

rx	Source is reachable through the interface on which the packet was received.
any	Source is reachable through any interface.
allow-default	(Optional) Allows the lookup table to match the default route and use the route for verification.
allow-self-ping	(Optional) Allows the router to ping a secondary address.
access-list-name	(Optional) Name of the IPv6 access list. Names cannot contain a space or quotation mark, or begin with a numeral.

Command Default

Unicast RPF is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Aggregation Services Routers.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

The **ipv6 verify unicast reverse-path** command is used to enable Unicast RPF for IPv6 in loose checking mode.

Use the **ipv6 verify unicast source reachable-via** command to mitigate problems caused by malformed or forged (spoofed) IP source addresses that pass through an IPv6 router. Malformed or forged source addresses can indicate denial-of-service (DoS) attacks based on source IPv6 address spoofing.

The URPF feature checks to see if any packet 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 URPF does not find a reverse path for the packet, U RPF can drop or forward the packet, depending on whether an access control list (ACL) is specified in the **ipv6 verify unicast source reachable-via** command. If an ACL is specified in the command, then when (and only when) a packet fails the URPF check, the ACL is checked to see if 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 U RPF drops and in the interface statistics for Unicast RPF.

If no ACL is specified in the **ipv6 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.

U RPF events can be logged by specifying the logging option for the ACL entries used by the **ipv6 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.

Examples

The following example enables Unicast RPF on any interface:

```
ipv6 verify unicast source reachable-via any
```

Related Commands

Command	Description
ipv6 access-list	Defines an IPv6 access list and places the router in IPv6 access list configuration mode.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 virtual-reassembly

To enable Virtual Fragment Reassembly (VFR) on an interface, use the **ipv6 virtual-reassembly** command in global configuration mode. To remove VFR configuration, use the **no** form of this command.

ipv6 virtual-reassembly [**in** | **out**] [**max-reassemblies** *maxreassemblies*] [**max-fragments** *max-fragments*] [**timeout** *seconds*] [**drop-fragments**]

no ipv6 virtual-reassembly [**in** | **out**] [**max-reassemblies** *maxreassemblies*] [**max-fragments** *max-fragments*] [**timeout** *seconds*] [**drop-fragments**]

Syntax Description

in	(Optional) Enables VFR on the ingress direction of the interface.
out	(Optional) Enables VFR on the egress direction of the interface.
max-reassemblies *maxreassemblies*	(Optional) Sets the maximum number of concurrent reassemblies (fragment sets) that the Cisco IOS software can handle at a time. The default value is 64.
max-fragments *max-fragments*	(Optional) Sets the maximum number of fragments allowed per datagram (fragment set). The default is 16.
timeout *seconds*	(Optional) Sets the timeout value of the fragment state. The default timeout value is 2 seconds. If a datagram does not receive all its fragments within 2 seconds, all of the fragments received previously will be dropped and the fragment state will be deleted.
drop-fragments	(Optional) Turns the drop fragments feature on or off.

Command Default

Max-reassemblies = 64
Fragments = 16
If neither the **in** or **out** keyword is specified, VFR is enabled on the ingress direction of the interface only.
drop-fragments keyword is not enabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(7)T	This command was introduced.
15.1(1)T	The **in** and **out** keywords were added. • The **out** keyword must be used to configure or disable the egress direction of the interface.
Cisco IOS XE Release 3.4S	The **drop-fragments** keyword was added.

Usage Guidelines

When the **ipv6 virtual-reassembly** command is configured on an interface without using one of the command keywords, VFR is enabled on the ingress direction of the interface only. In Cisco IOS XE Release 3.4S, all VFR-related alert messages are suppressed by default.

Maximum Number of Reassemblies

Whenever the maximum number of 256 reassemblies (fragment sets) is crossed, all the fragments in the forthcoming fragment set will be dropped and an alert message VFR-4-FRAG_TABLE_OVERFLOW will be logged to the syslog server.

Maximum Number of Fragments per Fragment Set

If a datagram being reassembled receives more than eight fragments then, tall fragments will be dropped and an alert message VFR-4-TOO_MANY_FRAGMENTS will be logged to the syslog server.

Explicit Removal of Egress Configuration

As of the Cisco IOS 15.1(1)T release, the **no ipv6 virtual-reassembly** command, when used without keywords, removes ingress configuration only. To remove egress interface configuration, you must enter the **out** keyword.

Examples

The following example configures the ingress direction on the interface. It sets the maximum number of reassemblies to 32, maximum fragments to 4, and the timeout to 7 seconds:

```
Router(config)# interface Ethernet 0/0
Router(config-if)# ipv6 virtual-reassembly max-reassemblies 32 max-fragments 4 timeout 7
```

The following example enables the VFR on the ingress direction of the interface. Note that even if the **in** keyword is not used, the configuration default is to configure the ingress direction on the interface:

```
Router(config)# interface Ethernet 0/0
Router(config-if)# ipv6 virtual-reassembly
Router(config-if)# end

Router# show run interface Ethernet 0/0

interface Ethernet0/0
no ip address
ipv6 virtual-reassembly in
```

The following example enables egress configuration on the interface. Note that the **out** keyword must be used to enable and disable egress configuration on the interface:

```
Router(config)# interface Ethernet 0/0
Router(config-if)# ipv6 virtual-reassembly out
Router(config-if)# end

Router# show run interface Ethernet 0/0

interface Ethernet0/0
no ip address
ipv6 virtual-reassembly out
end
```

The following example disables egress configuration on the interface:

```
Router(config)# interface Ethernet 0/0
Router(config-if)# no ipv6 virtual-reassembly out
Router(config-if)# end
```

ipv6 virtual-reassembly drop-fragments

To drop all fragments on an interface, use the **ipv6 virtual-reassembly drop-fragments** command in global configuration mode. Use the **no** form of this command to remove the packet-dropping behavior.

ipv6 virtual-reassembly drop-fragments

no ipv6 virtual-reassembly drop-fragments

Syntax Description

This command has no arguments or keywords.

Command Default

Fragments on an interface are not dropped.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Examples

The following example causes all fragments on an interface to be dropped:

```
ipv6 virtual-reassembly drop-fragments
```

isdn switch-type (BRI)

To specify the central office switch type on the ISDN interface, use the **isdn switch-type** command in global or interface configuration mode. To remove an ISDN switch type, use the **no** form of this command.

isdn switch-type *switch-type*

no isdn switch-type *switch-type*

Syntax Description

switch-type	ISDN service provider switch type. Table 33 in the "Usage Guidelines" section lists the supported switch types.

Defaults

No ISDN switch type is specified.

Command Modes

Global configuration or interface configuration

Note This command can be entered in either global configuration or interface configuration mode. When entered in global configuration mode, the **basic-qsig** switch type command specifies that the Cisco MC3810 use QSIG signaling on all BRI interfaces; when entered in interface configuration mode, the command specifies that an individual BRI voice interface use QSIG signaling. The interface configuration mode setting overrides the global configuration setting on individual interfaces.

Command History

Release	Modification
9.21	This command was introduced as a global command.
11.3 T	This command was introduced as an interface command.
12.0(3)XG	The **basic-qsig** and **primary-qsig s**witch type options were added to support BRI QSIG voice signaling.

Usage Guidelines

For the Cisco AS5300 access server, you have the choice of configuring the **isdn-switch-type** command to support Q.SIG in either global configuration mode or interface configuration mode. When entered in global configuration mode, the setting applies to the entire Cisco AS5300 access server. When entered in interface configuration mode, the setting applies only to the T1/E1 interface specified. The interface configuration mode setting overrides the global configuration setting.

For example, if you have a Q.SIG connection on one line as well as on the PRI port, you can configure the ISDN switch type in one of the following combinations:

- Set the global **isdn-switch-type** command to support Q.SIG and set the interface **isdn-switch-type** command for **interface serial 0:23** to a PRI setting such as 5ess.
- Set the global **isdn-switch-type** command to support PRI 5ess and set the interface **isdn-switch-type** command for **interface serial 1:23** to support Q.SIG.
- Configure the global **isdn-switch-type** command to another setting (such as switch type VN3), set the interface **isdn-switch-type** command for **interface serial 0:23** to a PRI setting, and set the interface **isdn-switch-type** command for **interface serial 1:23** to support Q.SIG.

For the Cisco MC3810 router, if you are using different Cisco MC3810 BRI port interfaces with different ISDN switch types, you can use global and interface commands in any combination, as long as you remember that interface commands always override a global command.

For example, if you have a BRI QSIG switch interface on BRI voice ports 1, 2, 3 and 4, but a BRI 5ess switch interface on BRI backup port 0, you can configure the ISDN switch types in any of the following combinations:

- Enter the **isdn switch-type basic-qsig global configuration command**, and enter the **isdn switch-type bri-5ess command** on interface 0.
- Enter the **isdn switch-type bri-5ess** global configuration command, and enter the **isdn switch-type basic-qsig command** on interfaces 1, 2, 3, and 4 individually.
- Enter the **isdn switch-type bri-5ess** command on interface 0, and enter the **isdn switch-type basic-qsig command** on interfaces 1, 2, 3, and 4 individually.

If you use the **no isdn switch-type** global configuration command, any switch type that was originally entered in global configuration mode is canceled; however, any switch type originally entered on an interface is not affected. If you use the **no isdn switch-type** interface configuration command, any switch type configuration on the interface is canceled.

Note In the Cisco MC3810, ISDN BRI voice ports support *only* switch type **basic-qsig**; ISDN BRI backup ports support all other listed switch types, but *not* **basic-qsig**.

Note The dial-peer **codec** command must be configured before any calls can be placed over the connection to the PINX. The default codec type is G729a.

If you are using the Multiple ISDN Switch Types feature to apply ISDN switch types to different interfaces, refer to the chapters “Configuring ISDN BRI” and “Configuring ISDN PRI” in the *Cisco IOS Dial Technologies Configuration Guide* for additional details.

The Cisco IOS command parser accepts the following switch types: basic-nwnet3, vn2, and basic-net3; however, when viewing the NVRAM configuration, the basic-net3 or vn3 switch types are displayed, respectively.

To remove an ISDN switch type from an ISDN interface, specify **the no isdn switch-type** *switch-type command*.

Table 33 lists supported BRI switch types by geographic area.

Table 33 ISDN Service Provider BRI Switch Types

Keywords by Area	Switch Type
Voice/PBX Systems	
basic-qsig	PINX (PBX) switches with QSIG signaling per Q.931
Australia, Europe, UK	
basic-1tr6	German 1TR6 ISDN switch
basic-net3	NET3 ISDN BRI for Norway NET3, Australia NET3, and New Zealand NET3switch types; ETSI-compliant switch types for Euro-ISDN E-DSS1 signaling system
vn3	French ISDN BRI switches
Japan	
ntt	Japanese NTT ISDN switches
North America	
basic-5ess	Lucent (AT&T) basic rate 5ESS switch
basic-dms100	Northern Telecom DMS-100 basic rate switch
basic-ni	National ISDN switches
All Users	
none	No switch defined

Examples

The following example configures the French VN3 ISDN switch type:

```
isdn switch-type vn3
```

The following example uses the Multiple ISDN Switch Types feature and shows use of the global ISDN switch type **basic-ni** keyword (formerly **basic-ni1**) and the **basic-net3** interface-level switch type keyword. ISDN switch type **basic-net3** is applied to BRI interface 0 and overrides the global switch setting.

```
isdn switch-type basic-ni
!
interface BRI0
 isdn switch-type basic-net3
```

The following example configures the Cisco MC3810 router to use BRI QSIG signaling for all of its BRI voice ports:

```
isdn switch-type basic-qsig
```

The following example configures the Cisco MC3810 to use BRI QSIG signaling for BRI voice port 1. On port 1, this setting overrides any different signaling set in the previous example.

```
interface bri 1
 isdn switch-type basic-qsig
```

isis ipv6 metric

To configure the value of an Intermediate System-to-Intermediate System (IS-IS) IPv6 metric, use the **isis ipv6 metric** command in interface configuration mode. To return the metric to its default value, use the **no** form of this command.

isis ipv6 metric {*metric-value* | **maximum**} [**level-1** | **level-2**]

no isis ipv6 metric {*metric-value* | **maximum**} [**level-1** | **level-2**]

Syntax Description

metric-value	Value added to the metric of an IPv6 IS-IS route received in a report message. The default metric value is 10. The range is from 1 to 16777214.
maximum	Excludes a link or adjacency from the Shortest Path Tree (SPF) calculation.
level-1	(Optional) Enables this command on routing Level 1. If no optional keyword is specified, the metric is enabled on routing Level 1 and Level 2.
level-2	(Optional) Enables this command on routing Level 2. If no optional keyword is specified, the metric is enabled on routing Level 1 and Level 2.

Command Default

The default metric value is set to 10.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.1	The **maximum** keyword was 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.
12.2(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 2.6	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The **isis ipv6 metric** command is used only in multitopology IS-IS.

Changing the metric allows differentiation between IPv4 and IPv6 traffic, forcing traffic onto different interfaces. This function allows you to use the lower-cost rather than the high-cost interface.

For using extended metrics, such as with the IS-IS multitopology for IPv6 feature, Cisco IOS software provides support of a 24-bit metric field, the so-called “wide metric.” Using the new metric style, link metrics now have a maximum value of 16777214 with a total path metric of 4261412864.

Cisco IOS Release 12.4(13) and 12.4(13)T

Entering the **maximum** keyword will exclude the link from the SPF calculation. If a link is advertised with the maximum link metric, the link will not be considered during the normal SPF computation. When the link excluded from the SPF, it will not be advertised for calculating the normal SPF. An example would be a link that is available for traffic engineering, but not for hop-by-hop routing. If a link, such as one that is used for traffic engineering, should not be included in the SPF calculation, enter the **isis ipv6 metric** command with the **maximum** keyword.

Note The **isis ipv6 metric maximum** command applies only when the **metric-style wide** command has been entered. The **metric-style wide** command is used to configure IS-IS to use the new-style type, length, value (TLV) because TLVs that are used to advertise IPv6 information in link-state packets (LSPs) are defined to use only extended metrics.

Examples

The following example sets the value of an IS-IS IPv6 metric to 20:

```
Router(config)# interface Ethernet 0/0/1
Router(config-if)# isis ipv6 metric 20
```

The following example sets the IS-IS IPv6 metric for the link to maximum. SPF will ignore the link for both Level 1 and Level 2 routing because neither the **level-1** keyword nor the **level-2** keyword was entered.

```
Router(config)# interface fastethernet 0/0
Router(config-if)# isis ipv6 metric maximum
```

Related Commands

Command	Description
metric-style wide	Configures a router running IS-IS so that it generates and accepts only new-style TLVs.

keepalive target

To identify Session Initiation Protocol (SIP) servers that will receive keepalive packets from the SIP gateway, use the **keepalive target** command in SIP user-agent configuration mode. To disable the **keepalive target** command behavior, use the **no** form of this command.

keepalive target {{**ipv4:***address* | **ipv6:***address*}[**:***port*] | **dns:***hostname*} | [**tcp** [**tls**]] | [**udp**] | [**secondary**]

no keepalive target [**secondary**]

Syntax Description

ipv4:*address*	IP address (in IP version 4 format) of the primary or secondary SIP server to monitor.
ipv6:*address*	IPv6 address of the primary or secondary SIP server to monitor.
:*port*	(Optional) SIP port number. Default SIP port number is 5060.
dns:hostname	DNS hostname of the primary or secondary SIP server to monitor.
tcp	(Optional) Sends keepalive packets over TCP.
tls	(Optional) Sends keepalive packets over Transport Layer Security (TLS).
udp	(Optional) Sends keepalive packets over User Datagram Protocol (UDP).
secondary	(Optional) Associates the IP version 4 address or the domain name system (DNS) hostname to a secondary SIP server to monitor.

Command Default

No keepalives are sent by default from SIP gateway to SIP gateway. The SIP port number is 5060 by default.

Command Modes

SIP user-agent configuration (config-sip-ua)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(22)T	Support for IPv6 was added.

Usage Guidelines

The primary or secondary SIP server addresses are in the following forms: dns:example.sip.com or ipv4:172.16.0.10.

Examples

The following example sets the primary SIP server address and defaults to the UDP transport:

```
sip-ua
 keepalive target ipv4:172.16.0.10
```

The following example sets the primary SIP server address and the transport to UDP:

```
sip-ua
 keepalive target ipv4:172.16.0.10 udp
```

The following example sets both the primary and secondary SIP server address and the transport to UDP:

```
sip-ua
 keepalive target ipv4:172.16.0.10 udp
 keepalive target ipv4:172.16.0.20 udp secondary
```

The following example sets both the primary and secondary SIP server addresses and defaults to the UDP transport:

```
sip-ua
 keepalive target ipv4:172.16.0.10
 keepalive target ipv4:172.16.0.20 secondary
```

The following example sets the primary SIP server address and the transport to TCP:

```
sip-ua
 keepalive target ipv4:172.16.0.10 tcp
```

The following example sets both the primary and secondary SIP server addresses and the transport to TCP:

```
sip-ua
 keepalive target ipv4:172.16.0.10 tcp
 keepalive target ipv4:172.16.0.20 tcp secondary
```

The following example sets the primary SIP server address and the transport to TCP and sets security to TLS mode:

```
sip-ua
 keepalive target ipv4:172.16.0.10 tcp tls
```

The following example sets both the primary and secondary SIP server addresses and the transport to TCP and sets security to the TLS mode:

```
sip-ua
 keepalive target ipv4:172.16.0.10 tcp tls
 keepalive target ipv4:172.16.0.20 tcp tls secondary
```

Related Commands

Command	Description
busyout monitor keepalive	Selects a voice port or ports to be busied out in cases of a keepalive failure.
keepalive trigger	Sets the trigger count to the number of Options message requests that must consecutively receive responses from the SIP servers in order to unbusy the voice ports when in the down state.
retry keepalive	Sets the retry keepalive count for retransmission.
timers keepalive	Sets the timers keepalive interval between sending Options message requests when the SIP server is active or down.

key

To identify an authentication key on a key chain, use the **key** command in key-chain configuration mode. To remove the key from the key chain, use the **no** form of this command.

key *key-id*

no key *key-id*

Syntax Description

key-id	Identification number of an authentication key on a key chain. The range of keys is from 0 to 2147483647. The key identification numbers need not be consecutive.

Command Default

No key exists on the key chain.

Command Modes

Key-chain configuration (config-keychain)

Command History

Release	Modification
11.1	This command was introduced.
12.4(6)T	Support for IPv6 was added.
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.

Usage Guidelines

Only DRP Agent, Enhanced Interior Gateway Routing Protocol (EIGRP), and Routing Information Protocol (RIP) Version 2 use key chains.

It is useful to have multiple keys on a key chain so that the software can sequence through the keys as they become invalid after time, based on the **accept-lifetime** and **send-lifetime** key chain key command settings.

Each key has its own key identifier, which is stored locally. The combination of the key identifier and the interface associated with the message uniquely identifies the authentication algorithm and Message Digest 5 (MD5) authentication key in use. Only one authentication packet is sent, regardless of the number of valid keys. The software starts looking at the lowest key identifier number and uses the first valid key.

If the last key expires, authentication will continue and an error message will be generated. To disable authentication, you must manually delete the last valid key.

To remove all keys, remove the key chain by using the **no key chain** command.

Examples

The following example configures a key chain named chain1. The key named key1 will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. The key named key2 will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or a discrepancy in the set time of the router. There is a 30-minute leeway on each side to handle time differences.

```
Router(config)# interface ethernet 0
Router(config-if)# ip rip authentication key-chain chain1
Router(config-if)# ip rip authentication mode md5
!
Router(config)# router rip
Router(config-router)# network 172.19.0.0
Router(config-router)# version 2
!
Router(config)# key chain chain1
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string key1
Router(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 14:00:00 Jan 25 1996 duration 3600
Router(config-keychain-key)# exit
Router(config-keychain)# key 2
Router(config-keychain-key)# key-string key2
Router(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 15:00:00 Jan 25 1996 duration 3600
```

The following named configuration example configures a key chain named chain1 for EIGRP address-family. The key named key1 will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. The key named key2 will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or a discrepancy in the set time of the router. There is a 30-minute leeway on each side to handle time differences.

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# network 10.0.0.0
Router(config-router-af)# af-interface ethernet0/0
Router(config-router-af-interface)# authentication key-chain trees
Router(config-router-af-interface)# authentication mode md5
Router(config-router-af-interface)# exit
Router(config-router-af)# exit
Router(config-router)# exit
Router(config)# key chain chain1
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string key1
Router(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 14:00:00 Jan 25 1996 duration 3600
Router(config-keychain-key)# exit
Router(config-keychain)# key 2
Router(config-keychain-key)# key-string key2
Router(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 15:00:00 Jan 25 1996 duration 3600
```

The following named configuration example configures a key chain named chain1 for EIGRP service-family. The key named key1 will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. The key named key2 will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or a discrepancy in the set time of the router. There is a 30-minute leeway on each side to handle time differences.

```
Router(config)# eigrp virtual-name
Router(config-router)# service-family ipv4 autonomous-system 4453
Router(config-router-sf)# network 10.0.0.0
Router(config-router-sf)# sf-interface ethernet0/0
```

```
Router(config-router-sf-interface)# authentication key-chain trees
Router(config-router-sf-interface)# authentication mode md5
Router(config-router-sf-interface)# exit
Router(config-router-sf)# exit
Router(config-router)# exit
Router(config)# key chain chain1
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string key1
Router(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 14:00:00 Jan 25 1996 duration 3600
Router(config-keychain-key)# exit
Router(config-keychain)# key 2
Router(config-keychain-key)# key-string key2
Router(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 15:00:00 Jan 25 1996 duration 3600
```

Related Commands

Command	Description
accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.
ip authentication key-chain eigrp	Enables authentication of EIGRP packets.
key chain	Defines an authentication key chain needed to enable authentication for routing protocols.
key-string (authentication)	Specifies the authentication string for a key.
send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.
show key chain	Displays authentication key information.

key (TACACS+)

To configure the per-server encryption key on the TACACS+ server, use the **key** command in TACACS+ server configuration mode. To remove the per-server encryption key, use the **no** form of this command.

key [**0** | **7**] *key-string*

no key [**0** | **7**] *key-string*

Syntax Description

0	(Optional) Specifies that an unencrypted key will follow.
7	(Optional) Specifies that a hidden key will follow.
key-string	Unencrypted shared key.

Command Default

No TACACS+ encryption key is configured.

Command Modes

TACACS+ server configuration (config-server-tacacs)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines

The **key** command allows you to configure a per-server encryption key.

Examples

The following example shows how to specify an unencrypted shared key named key1:

```
Router (config)# tacacs server server1
Router(config-server-tacacs)# key 0 key1
```

Related Commands

Command	Description
tacacs server	Configures the TACACS+ server for IPv6 or IPv4 and enters TACACS+ server configuration mode.

key chain

To define an authentication key chain needed to enable authentication for routing protocols and enter key-chain configuration mode, use the **key chain** command in global configuration mode. To remove the key chain, use the **no** form of this command.

key chain *name-of-chain*

no key chain *name-of-chain*

Syntax Description

name-of-chain	Name of a key chain. A key chain must have at least one key and can have up to 2147483647 keys.

Command Default

No key chain exists.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.1	This command was introduced.
12.4(6)T	Support for IPv6 was added.
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.

Usage Guidelines

Only DRP Agent, Enhanced Interior Gateway Routing Protocol (EIGRP), and Routing Information Protocol (RIP) Version 2 use key chains.

You must configure a key chain with keys to enable authentication.

Although you can identify multiple key chains, we recommend using one key chain per interface per routing protocol. Upon specifying the **key chain** command, you enter key chain configuration mode.

Examples

The following example configures a key chain named chain1. The key named key1 will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. The key named key2 will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or a discrepancy in the set time of the router. There is a 30-minute leeway on each side to handle time differences.

```
Router(config)# interface ethernet 0
Router(config-if)# ip rip authentication key-chain chain1
Router(config-if)# ip rip authentication mode md5
!
```

```
Router(config)# router rip
Router(config-router)# network 172.19.0.0
Router(config-router)# version 2
!
Router(config)# key chain chain1
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string key1
Router(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 14:00:00 Jan 25 1996 duration 3600
Router(config-keychain-key)# exit
Router(config-keychain)# key 2
Router(config-keychain-key)# key-string key2
Router(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 15:00:00 Jan 25 1996 duration 3600
```

The following named configuration example configures a key chain named chain1 for EIGRP address-family. The key named key1 will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. The key named key2 will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or a discrepancy in the set time of the router. There is a 30-minute leeway on each side to handle time differences.

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# network 10.0.0.0
Router(config-router-af)# af-interface ethernet0/0
Router(config-router-af-interface)# authentication key-chain trees
Router(config-router-af-interface)# authentication mode md5
Router(config-router-af-interface)# exit
Router(config-router-af)# exit
Router(config-router)# exit
Router(config)# key chain chain1
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string key1
Router(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 14:00:00 Jan 25 1996 duration 3600
Router(config-keychain-key)# exit
Router(config-keychain)# key 2
Router(config-keychain-key)# key-string key2
Router(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 15:00:00 Jan 25 1996 duration 3600
```

The following named configuration example configures a key chain named trees for service-family. The key named chestnut will be accepted from 1:30 pm to 3:30 pm and be sent from 2:00 pm to 3:00 pm. The key birch will be accepted from 2:30 pm to 4:30 pm and be sent from 3:00 pm to 4:00 pm. The overlap allows for migration of keys or a discrepancy in the set time of the router. There is a 30-minute leeway on each side to handle time differences.

```
Router(config)# router eigrp virtual-name
Router(config-router)# service-family ipv4 autonomous-system 4453
Router(config-router-sf)# sf-interface ethernet
Router(config-router-sf-interface)# authentication key chain trees
Router(config-router-sf-interface)# authentication mode md5
Router(config-router-sf-interface)# exit
Router(config-router-sf)# exit
Router(config-router)# exit
Router(config)# key chain chain1
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string chestnut
Router(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 14:00:00 Jan 25 1996 duration 3600
Router(config-keychain-key)# exit
Router(config-keychain)# key 2
Router(config-keychain-key)# key-string birch
```

```
Router(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 15:00:00 Jan 25 1996 duration 3600
```

Related Commands

Command	Description
accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.
ip rip authentication key-chain	Enables authentication for RIP Version 2 packets and specifies the set of keys that can be used on an interface.
ip authentication key-chain eigrp	Enables authentication of EIGRP packets.
key	Identifies an authentication key on a key chain.
key-string (authentication)	Specifies the authentication string for a key.
send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.
show key chain	Displays authentication key information.

key-string (authentication)

To specify the authentication string for a key, use the **key-string** (authentication) command in key chain key configuration mode. To remove the authentication string, use the **no** form of this command.

key-string *text*

no key-string *text*

Syntax Description

text	Authentication string that must be sent and received in the packets using the routing protocol being authenticated. The string can contain from 1 to 80 uppercase and lowercase alphanumeric characters, except that the first character cannot be a number.

Command Default

No authentication string for a key exists.

Command Modes

Key chain key configuration (config-keychain-key)

Command History

Release	Modification
11.1	This command was introduced.
12.4(6)T	Support for IPv6 was added.
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.

Usage Guidelines

Only DRP Agent, Enhanced Interior Gateway Routing Protocol (EIGRP), and Routing Information Protocol (RIP) Version 2 use key chains. Each key can have only one key string.

If password encryption is configured (with the **service password-encryption** command), the software saves the key string as encrypted text. When you write to the terminal with the **more system:running-config** command, the software displays key-string 7 encrypted text.

Examples

The following example configures a key chain named chain1. The key named key1 will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. The key named key2 will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or a discrepancy in the set time of the router. There is a 30-minute leeway on each side to handle time differences.

```
Router(config)# interface ethernet 0
Router(config-if)# ip rip authentication key-chain chain1
Router(config-if)# ip rip authentication mode md5
!
Router(config)# router rip
Router(config-router)# network 172.19.0.0
Router(config-router)# version 2
```

```
!
Router(config)# key chain chain1
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string key1
Router(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 14:00:00 Jan 25 1996 duration 3600
Router(config-keychain-key)# exit
Router(config-keychain)# key 2
Router(config-keychain-key)# key-string key2
Router(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 15:00:00 Jan 25 1996 duration 3600
```

The following example configures a key chain named chain1 for EIGRP address-family. The key named key1 will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. The key named key2 will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or a discrepancy in the set time of the router. There is a 30-minute leeway on each side to handle time differences.

```
Router(config)# eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# network 10.0.0.0
Router(config-router-af)# af-interface ethernet0/0
Router(config-router-af-interface)# authentication key-chain trees
Router(config-router-af-interface)# authentication mode md5
Router(config-router-af-interface)# exit
Router(config-router-af)# exit
Router(config-router)# exit
Router(config)# key chain chain1
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string key1
Router(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 14:00:00 Jan 25 1996 duration 3600
Router(config-keychain-key)# exit
Router(config-keychain)# key 2
Router(config-keychain-key)# key-string key2
Router(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 15:00:00 Jan 25 1996 duration 3600
```

Related Commands

Command	Description
accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.
ip authentication key-chain eigrp	Enables authentication of EIGRP packets.
key	Identifies an authentication key on a key chain.
key chain	Defines an authentication key-chain needed to enable authentication for routing protocols.
send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.
service password-encryption	Encrypts passwords.
show key chain	Displays authentication key information.

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 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.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

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.

limit address-count

To limit the number of IPv6 addresses allowed to be used on the port, use the **limit address-count** command in Neighbor Discovery Protocol (NDP) inspection policy configuration mode.

limit address-count *maximum*

Syntax Description

maximum	Sets the role of the device to host.

Command Default

The device role is host.

Command Modes

ND inspection policy configuration (config-nd-inspection)
RA guard policy configuration (config-ra-guard)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

The **limit address-count** command limits the number of IPv6 addresses allowed to be used on the port on which the policy is applied. Limiting the number of IPv6 addresses on a port helps limit the binding table size.

Use the **limit address-count** command after enabling NDP inspection policy configuration mode using the **ipv6 nd inspection policy** command.

Examples

The following example defines an NDP policy name as policy1, places the router in NDP inspection policy configuration mode, and limits the number of IPv6 addresses allowed on the port to 25:

```
Router(config)# ipv6 nd inspection policy policy1
Router(config-nd-inspection)# limit address-count 25
```

Related Commands

Command	Description
ipv6 nd inspection policy	Defines the NDP inspection policy name and enters NDP inspection policy configuration mode.
ipv6 nd raguard policy	Defines the RA guard policy name and enter RA guard policy configuration mode.

log-adjacency-changes

To configure the router to send a syslog message when an Open Shortest Path First (OSPF) neighbor goes up or down, use the **log-adjacency-changes** command in router configuration mode. To turn off this function, use the **no** form of this command.

log-adjacency-changes [**detail**]

no log-adjacency-changes [**detail**]

Syntax Description

detail	(Optional) Sends a syslog message for each state change, not just when a neighbor goes up or down.

Command Default

Enabled

Command Modes

Router configuration (config-router)

Command History

Release	Modification
11.2	This command was introduced as **ospf log-adjacency-changes**.
12.1	The **ospf** keyword was omitted and the **detail** keyword was added.
12.2(15)T	Support for IPv6 was added.
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.
15.1(2)S	This command was integrated into Cisco IOS Release 15.1(2)S.

Usage Guidelines

This command allows you to know about OSPF neighbors going up or down without turning on the **debug ip ospf packet** command or the **debug ipv6 ospf adjacency** command. The **log-adjacency-changes** command provides a higher level view of those changes of the peer relationship with less output than the **debug** command provides. The **log-adjacency-changes** command is on by default but only up/down (full/down) events are reported, unless the **detail** keyword is also used.

Examples

The following example configures the router to send a syslog message when an OSPF neighbor state changes:

```
log-adjacency-changes detail
```

Related Commands

Command	Description
debug ip ospf packet	Displays information about each OSPF packet received for IPv4.
debug ipv6 ospf	Displays debugging information for OSPF for IPv6.

log-adjacency-changes (OSPFv3)

To configure the router to send a syslog message when an Open Shortest Path First version 3 (OSPFv3) neighbor goes up or down, use the **log-adjacency-changes** command in router configuration mode. To turn off this function, use the **no** form of this command.

log-adjacency-changes [**detail**]

no log-adjacency-changes [**detail**]

Syntax Description

detail	(Optional) Sends a syslog message for each state change, not just when a neighbor goes up or down.

Command Default

This feature is enabled

Command Modes

OSPFv3 router configuration mode (config-router)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

Use the **log-adjacency changes** command to notify you when OSPFv3 neighbors go up or down. The **log-adjacency-changes** command provides a higher level view of those changes of the peer relationship with less output than **debug** commands provide. The **log-adjacency-changes** command is on by default, but only up/down (full/down) events are reported unless the **detail** keyword is also used.

Examples

The following example configures the router to send a syslog message when an OSPFv3 neighbor state changes:

```
Router(config-router)# log-adjacency-changes
```

Related Commands

Command	Description
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

logging event link-status (interface configuration)

To enable link-status event messaging on an interface, use the **logging event link-status** command in interface configuration mode. To disable link-status event messaging, use the **no** form of this command.

logging event link-status [**bchan** | **dchan** | **nfas**]

no logging event link-status [**bchan** | **dchan** | **nfas**]

Syntax Description

bchan	(Optional) Logs B-channel status messages. This keyword is available only for integrated services digital network (ISDN) serial interfaces.
dchan	(Optional) Logs D-channel status messages. This keyword is available only for ISDN serial interfaces.
nfas	(Optional) Logs non-facility associated signaling (NFAS) D-channel status messages. This keyword is available only for ISDN serial interfaces.

Command Default

Interface state-change messages are not sent.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(14)SX	This command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	This command was modified to support the Supervisor Engine 2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

To enable system logging of interface state-change events on a specific interface, enter the **logging event link-status** command.

Examples

The following example shows how to enable link-status event messaging on an interface:

```
Router(config-if)# logging event link-status
```

This example shows how to disable link-status event messaging on an interface:

```
Router(config-if)# no logging event link-status
```

logging host

To log system messages and debug output to a remote host, use the **logging host** command in global configuration mode. To remove a specified logging host from the configuration, use the **no** form of this command.

logging host {{*ip-address* | *hostname*} [**vrf** *vrf-name*] | **ipv6** {*ipv6-address* | *hostname*}} [**discriminator** *discr-name* | [[**filtered** [**stream** *stream-id*] | **xml**]] [**transport** {[**beep** [**audit**] [**channel** *chnl-number*] [**sasl** *profile-name*] [**tls cipher** [*cipher-num*] **trustpoint** *trustpt-name*]]] | **tcp** [**audit**] | **udp**} [**port** *port-num*]] [**sequence-num-session**] [**session-id** {**hostname** | **ipv4** | **ipv6** | **string** *custom-string*}]

no logging host {{*ip-address* | *hostname*} | **ipv6** {*ipv6-address* | *hostname*}}

Syntax Description

ip-address	IP address of the host that will receive the system logging (syslog) messages.
hostname	Name of the IP or IPv6 host that will receive the syslog messages.
vrf	(Optional) Specifies a virtual private network (VPN) routing and forwarding instance (VRF) that connects to the syslog server host.
vrf-name	(Optional) Name of the VRF that connects to the syslog server host.
ipv6	Indicates that an IPv6 address will be used for a host that will receive the syslog messages.
ipv6-address	IPv6 address of the host that will receive the syslog messages.
discriminator	(Optional) Specifies a message discriminator for the session.
discr-name	(Optional) Name of the message discriminator.
filtered	(Optional) Specifies that logging messages sent to this host should first be filtered by the Embedded Syslog Manager (ESM) syslog filter modules specified in the **logging filter** commands.
stream	(Optional) Specifies that only ESM filtered messages with the stream identification number specified in the *stream-id* argument should be sent to this host.
stream-id	(Optional) Number from 10 to 65535 that identifies the message stream.
xml	(Optional) Specifies that the logging output should be tagged using the Extensible Markup Language (XML) tags defined by Cisco.
transport	(Optional) Method of transport to be used. UDP is the default.
beep	(Optional) Specifies that the Blocks Extensible Exchange Protocol (BEEP) transport will be used.
audit	(Optional) Available only for BEEP and TCP. When the **audit** keyword is used, the specified host is identified for firewall audit logging.
channel	(Optional) Specifies the BEEP channel number to use.
chnl-number	(Optional) Number of the BEEP channel. Valid values are 1, 3, 5, 7, 9, 11, 13, and 15. The default is 1.
sasl	(Optional) Applies the Simple Authentication and Security Layer BEEP profile.
profile-name	(Optional) Name of the SASL profile.

tls cipher	(Optional) Specifies the cipher suites to be used for a connection. Cipher suites are referred to by mask values. Multiple cipher suites can be chosen by adding the mask values. The **tls cipher** *cipher-num* keyword and argument pair is available only in crypto images.
cipher-num	(Optional) Integer from 32 to 224 that is the mask value of a cipher suite (sum of up to three numbers: 32, 64, and 128) and refers to the following: ENC_FLAG_TLS_RSA_WITH_NULL_SHA – 32 ENC_FLAG_TLS_RSA_WITH_RC4_128_MD5 – 64 ENC_FLAG_TLS_RSA_WITH_AES_128_CBC_SHA – 128 The **tls cipher** *cipher-num* keyword and argument pair is available only in crypto images.
trustpoint	(Optional) Specifies a trustpoint for identity information and certificates. The **trustpoint** *trustpt-name* keyword and argument pair is available only in crypto images.
trustpt-name	(Optional) Name of the trustpoint. If you previously declared the trustpoint and want only to update its characteristics, specify the name you previously created. The **trustpoint** *trustpt-name* keyword and argument pair is available only in crypto images.
tcp	(Optional) Specifies that the TCP transport will be used.
udp	(Optional) Specifies that the User Datagram Protocol (UDP) transport will be used.
port	(Optional) Specifies that a port will be used.
port-number	(Optional) Integer from 1 through 65535 that defines the port. If a port number is not specified, the standard Cisco default port number for TCP is 601, for BEEP is 601, and for UDP is 514.
sequence-num-session	(Optional) Includes a session sequence number tag in the syslog message.
session-id	(Optional) Specifies syslog message session ID tagging.
hostname	Includes the hostname in the session ID tag.
ipv4	Includes the logging source IP address in the session ID tag.
ipv6	Includes the logging source IPv6 address in the session ID tag.
string	Includes the custom string in the session ID tag.
custom-string	Custom string in the s_id="custom_string" tag.

Command Default

System logging messages are not sent to any remote host.
When this command is entered without the **xml** or **filtered** keyword, messages are sent in the standard format.

Command Modes

Global configuration (config)

Command History

T Release	Modifications
10.0	The **logging** command was introduced.

12.2(15)T	The **logging host** command replaced the **logging** command. The **xml** keyword was added.
12.3(2)T	The **filtered** [**stream** *stream-id*] syntax was added as part of the ESM feature.
12.3(14)T	The **transport** keyword was added.
12.4(4)T	The **ipv6** *ipv6-address* keyword-argument pair was added.
12.4(11)T	Support for BEEP and the **discriminator**, **sequence-num-session**, and **session-id** keywords and *discr-name* argument were added.
S Release	**Modifications**
12.0(14)S	The **logging host** command replaced the **logging** command.
12.0(14)ST	The **logging host** command replaced the **logging** command.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S and the **vrf** *vrf-name* keyword-argument pair was added.
SR Release	**Modifications**
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA. The **vrf** *vrf-name* and **xml** keywords were supported.
SX Release	**Modifications**
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH. The **vrf** *vrf-name* and **xml** keywords were supported.
12.2(33)SXI	Support for BEEP and the **discriminator**, **sequence-num-session**, and **session-id** keywords and *discr-name* argument were added.
XE Release	**Modifications**
12.3(2)XE	This command was integrated into Cisco IOS Release 12.3(2)XE.
SB Release	**Modifications**
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB. The **vrf** *vrf-name* and **xml** keywords were supported.
12.2(31)SB2	This command was implemented on the Cisco 10000 series routers. The **vrf** *vrf-name* and **xml** keywords were supported.

Usage Guidelines

Standard system logging is enabled by default. If logging is disabled on your system (using the **no logging on** command), you must enter the **logging on** command to reenable logging before you can use the **logging host** command.

The **logging host** command identifies a remote host (usually a device serving as a syslog server) to receive logging messages. By issuing this command more than once, you can build a list of hosts that receive logging messages.

To specify the severity level for logging to all hosts, use the **logging trap** command.

Use the **vrf** *vrf-name* keyword and argument to enable a syslog client (a provider edge [PE] router) to send syslog messages to a syslog server host connected through a VRF interface. To delete the configuration of the syslog server host from the VRF, use the **no logging host** command with the **vrf** *vrf-name* keyword and argument.

When XML-formatted syslog is enabled using the **logging host** command with the **xml** keyword, messages are sent to the specified host with the system-defined XML tags. These tags are predefined and cannot be configured by a user. XML formatting is not applied to debug output.

If you are using the ESM feature, you can enable ESM-filtered syslog messages to be sent to one or more hosts using the **logging host filtered** command. To use the ESM feature, you must first specify the syslog filter modules that should be applied to the messages using the **logging filter** command. See the description of the **logging filter** command for more information about the ESM feature.

Note ESM and message discriminator usage are mutually exclusive on a given syslog session.

Using the BEEP transport protocol, you can have reliable and secure delivery for syslog messages and configure multiple sessions over eight BEEP channels. The **sasl** *profile-name*, **tls cipher** *cipher-num,* **trustpoint** *trustpt-name* keywords and arguments are available only in crypto images.

To configure standard logging to a specific host after configuring XML-formatted or ESM-filtered logging to that host, use the **logging host** command without the **xml** or **filtered** keyword. Issuing the standard **logging host** command replaces an XML- or ESM- filtered **logging host** command, and vice versa, if the same host is specified.

You can configure the system to send standard messages to one or more hosts, XML-formatted messages to one or more hosts, and ESM-filtered messages to one or more hosts by repeating this command as many times as desired with the appropriate syntax. (See the "Examples" section.)

When the **no logging host** command is issued with or without the optional keywords, all logging to the specified host is disabled.

Examples

In the following example, messages at severity levels 0 (emergencies) through 5 (notifications) (**logging trap** command severity levels) are logged to a host at 192.168.202.169:

```
Router(config)# logging host 192.168.202.169
Router(config)# logging trap 5
```

In the following example, standard system logging messages are sent to the host at 192.168.200.225, XML-formatted system logging messages are sent to the host at 192.168.200.226, ESM-filtered logging messages with the stream 10 value are sent to the host at 192.168.200.227, and ESM-filtered logging messages with the stream 20 value are sent to host at 192.168.202.129:

```
Router(config)# logging host 192.168.200.225
Router(config)# logging host 192.168.200.226 xml
Router(config)# logging host 192.168.200.227 filtered stream 10
Router(config)# logging host 192.168.202.129 filtered stream 20
```

In the following example, messages are logged to a host with an IP address of 172.16.150.63 connected through a VRF named vpn1:

```
Router(config)# logging host 172.16.150.63 vrf vpn1
```

In the following example, the default UDP on an IPv6 server is set because no port number is specified. The default port number of 514 is used:

```
Router(config)# logging host ipv6 AAAA:BBBB:CCCC:DDDD::FFFF
```

In the following example, TCP port 1774 on an IPv6 server is set:

```
Router(config)# logging host ipv6 BBBB:CCCC:DDDD:FFFF::1234 transport tcp port 1774
```

In the following example, the UDP port default is used on an IPv6 server with a hostname of v6-hostname:

```
Router(config)# logging host ipv6 v6-hostname transport udp port 514
```

In the following example, a message discriminator named fltr1 is specified as well as the BEEP protocol for port 600 and channel 3.

```
Router(config)# logging host host2 dicriminator fltr1 transport beep channel 3 port 600
```

Related Commands

Command	Description
logging filter	Specifies a syslog filter module to be used by the ESM.
logging on	Globally controls (enables or disables) system message logging.
logging trap	Limits messages sent to the syslog servers based on severity level.
show logging	Displays the state of system message logging, followed by the contents of the standard syslog buffer.
show logging xml	Displays the state of XML-formatted system message logging, followed by the contents of the XML syslog buffer.

logging origin-id

To add an origin identifier to system logging messages sent to remote hosts, use the **logging origin-id** command in global configuration mode. To disable the origin identifier, use the **no** form of this command.

logging origin-id {**hostname** | **ip** | **ipv6** | **string** *user-defined-id*}

no logging origin-id

Syntax Description

hostname	Specifies that the hostname will be used as the message origin identifier.
ip	Specifies that the IP address of the sending interface will be used as the message origin identifier.
ipv6	Specifies that the IPv6 address of the sending interface will be used as the message origin identifier.
string *user-defined-id*	Allows you to enter your own identifying description. The *user-defined-id* argument is a string you specify. • You can enter a string with no spaces or use delimiting quotation marks to enclose a string with spaces.

Command Default

This command is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.3(1)	The **string** *user-defined-id* syntax was added.
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.
12.4(4)T	The **ipv6** keyword was added.
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.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

The origin identifier is added to the beginning of all system logging (syslog) messages sent to remote hosts. The identifier can be the hostname, the IP address, the IPv6 address, or any text that you specify. The origin identifier is not added to messages sent to local destinations (the console, monitor, or buffer).

The origin identifier is useful for identifying the source of system logging messages in cases where you send syslog output from multiple devices to a single syslog host.

When you specify your own identification string using the **logging origin-id string** *user-defined-id* command, the system expects a string without spaces. For example:

```
Router(config)# logging origin-id string Cisco_Systems
```

To use spaces (multiple words) or additional syntax, enclose the string with quotation marks (“ ”). For example:

```
Router(config)# logging origin-id string "Cisco Systems, Inc."
```

Examples

In the following example, the origin identifier “Domain 1, router B” will be added to the beginning of all system logging messages sent to remote hosts:

```
Router(config)# logging origin-id string Domain 1, router B
```

In the following example, all logging messages sent to remote hosts will have the IP address configured for serial interface 1 added to the beginning of the message:

```
Router(config)# logging host 209.165.200.225
Router(config)# logging trap 5
Router(config)# logging source-interface serial 1
Router(config)# logging origin-id ip
```

Related Commands

Command	Description
logging host	Enables system message logging to a remote host.
logging source-interface	Forces logging messages to be sent from a specified interface, instead of any available interface.
logging trap	Configures the severity level at or numerically below which logging messages should be sent to a remote host.

logging source-interface

To specify the source IPv4 or IPv6 address of system logging packets, use the **logging source-interface** command in global configuration mode. To remove the source designation, use the **no** form of this command.

logging source-interface *type number* **vrf** *vrf_name*

no logging source-interface

Syntax Description

type number	Interface type and number.
vrf *vrf_name*	Name of VRF.

Command Default

The wildcard interface address is used.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2	This command was introduced.
12.4(4)T	This command was modified. IPv6 support 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. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SXJ1	This command was modified to include the **vrf** keyword and attribute.
15.1(3)S	This command was modified to include the **vrf** keyword and attribute.

Usage Guidelines

This command can be configured on the Virtual Routing and Forwarding (VRF) and non-VRF interfaces. Normally, a syslog message contains the IPv4 or IPv6 address of the interface used to exit the router. The **logging source-interface** command configures the syslog packets that contain the IPv4 or IPv6 address of a particular interface, regardless of which interface the packet uses to exit the router.

When no specific interface is configured, a wildcard interface address of 0.0.0.0 (for IPv4) or :: (for IPv6) is used, and the IP socket selects the best outbound interface.

If you configure the same VRF interface multiple times the newest configuration will override earlier configurations.

The maximum allowable source-interfaces commands is 200 since there can be only a maximum of 200 hosts.

Examples

The following example shows how to specify that the IP address of Ethernet interface 0 is the source IP address for all syslog messages:

```
Router(config)# logging source-interface ethernet 0
```

The following example shows how to specify the IP address for Ethernet interface 2/1 is the source IP address for all syslog messages:

```
Router(config)# logging source-interface ethernet 2/1
```

The following sample output displays that the **logging source-interface** command is configured on a VRF source interface:

```
Router# show running interface loopback49
            Building configuration...

            Current configuration : 84 bytes
            !
            interface Loopback49
             ip vrf forwarding black
             ip address 49.0.0.1 255.0.0.0
            end
Router# show running | includes logging
      logging source-interface Loopback49 vrf black
      logging host 130.0.0.1 vrf black
```

Related Commands

Command	Description
logging	Logs messages to a syslog server host.

log-neighbor-changes (IPv6 EIGRP)

To enable the logging of changes in Enhanced Interior Gateway Routing Protocol (EIGRP) IPv6 neighbor adjacencies, use the **log-neighbor-changes** command in router configuration mode. To disable the logging of changes in EIGRP IPv6 neighbor adjacencies, use the **no** form of this command.

log-neighbor-changes

no log-neighbor-changes

Syntax Description

This command has no arguments or keywords.

Command Default

Adjacency changes are logged.

Command Modes

Router configuration

Command History

Release	Modification
12.4(6)T	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.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The **log-neighbor-changes** command enables the logging of neighbor adjacency changes to monitor the stability of the routing system and to help detect problems.

Logging is enabled by default. To disable the logging of neighbor adjacency changes, use the **no** form of this command.

Examples

The following example disables logging of neighbor changes for EIGRP process 1:

```
ipv6 router eigrp 1
 no log-neighbor-changes
```

The following configuration enables logging of neighbor changes for EIGRP process 1:

```
ipv6 router eigrp 1
 log-neighbor-changes
```

Related Commands

Command	Description
log-neighbor-warnings	Enables the logging of EIGRP neighbor warning messages.

log-neighbor-warnings

Note Effective with Cisco IOS Release 15.0(1)M, 12.2(33)SRE and Cisco IOS XE Release 2.5, the **log-neighbor-warnings** command was replaced by the **eigrp log-neighbor-warnings** command for IPv4 and IPv6 configurations. The **log-neighbor-warnings** command is still available for IPX configurations.

To enable the logging of Enhanced Interior Gateway Routing Protocol (EIGRP) neighbor warning messages, use the **log-neighbor-warnings** command in router configuration mode. To disable the logging of EIGRP neighbor warning messages, use the **no** form of this command.

log-neighbor-warnings [*seconds*]

no **log-neighbor-warnings**

Syntax Description

seconds	(Optional) The time interval (in seconds) between repeated neighbor warning messages. The range of seconds is from 1 through 65535.

Command Default

Neighbor warning messages are logged.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
12.4(6)T	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.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.0(1)M	This command was replaced by the **eigrp log-neighbor-warnings** command for IPv4 and IPv6 configurations. The **log-neighbor-warnings** command is still available for IPX configurations.
12.2(33)SRE	This command was replaced by the **eigrp log-neighbor-warnings** command for IPv4 and IPv6 configurations. The **log-neighbor-warnings** command is still available for IPX configurations.
Cisco IOS XE Release 2.5	This command was replaced by the **eigrp log-neighbor-warnings** command for IPv4 and IPv6 configurations. The **log-neighbor-warnings** command is still available for IPX configurations.

Usage Guidelines

When neighbor warning messages occur, they are logged by default. With the **log-neighbor-warnings** command, you can disable and enable the logging of neighbor warning messages and configure the interval between repeated neighbor warning messages.

Examples

The following example shows that neighbor warning messages will be logged for EIGRP process 1 and warning messages will be repeated in 5-minute (300 seconds) intervals:

```
Router(config)# ipv6 router eigrp 1
Router(config-router)# log-neighbor-warnings 300
```

Related Commands

Command	Description
log-neighbor-changes	Enables the logging of changes in EIGRP neighbor adjacencies.

managed-config-flag

To verify the advertised managed address configuration parameter, use the **managed-config-flag** command in router advertisement (RA) guard policy configuration mode.

managed-config-flag {**on** | **off**}

Syntax Description

on	Verification is enabled.
off	Verification is disabled.

Command Default

Verification is not enabled.

Command Modes

RA guard policy configuration (config-ra-guard)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

The **managed-config-flag** command enables verification of the advertised managed address configuration parameter (or "M" flag). This flag could be set by an attacker to force hosts to obtain addresses through a potentially untrusted DHCPv6 server.

Examples

The following example defines an RA guard policy name as raguard1, places the router in RA guard policy configuration mode, and enables M flag verification:

```
Router(config)# ipv6 nd raguard policy raguard1
Router(config-ra-guard)# managed-config-flag on
```

Related Commands

Command	Description
ipv6 nd raguard policy	Defines the RA guard policy name and enter RA guard policy configuration mode.

mask

To specify the destination or source mask, use the **mask** command in aggregation cache configuration mode. To disable the destination mask, use the **no** form of this command.

mask {**destination** | **source**} **minimum** *value*

no mask destination minimum *value*

Syntax Description

destination	Specifies that the destination mask is to be used for determining the aggregation cache.
source	Specifies that the source mask is to be used for determining the aggregation cache.
value	Specifies the number of bits to record from the source or destination mask. Range is from 1 to 32.

Command Default

The default value of the minimum mask is zero.

Command Modes

Aggregation cache configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.
12.3(7)T	Support was added for IPv6 source and destination addresses to be used for cache aggregation.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)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

This command is only available with router-based aggregation. Minimum masking capability is not available if router-based aggregation is not enabled.

Examples

The following example shows how to configure the mask to use the destination-prefix as the aggregation cache scheme with a minimum mask value of 32:

```
Router(config)# ipv6 flow-aggregation cache destination-prefix
Router(config-flow-cache)# mask destination minimum 32
```

Related Commands

Command	Description
ip flow-aggregation cache	Enables aggregation cache configuration mode.
ipv6 flow-aggregation cache	Enables aggregation cache configuration mode for IPv6 traffic.

Command	Description
show ip cache flow aggregation	Displays the aggregation cache configuration.
show ipv6 cache flow aggregation	Displays the aggregation cache configuration for IPv6 NetFlow configurations.

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 access-group name

To specify the name of an IPv6 access list against whose contents packets are checked to determine if they belong to the traffic class, use the **match access-group name** command in class-map configuration mode. To remove the name of the IPv6 access list, use the **no** form of this command.

match access-group name *ipv6-access-group*

no match access-group name *ipv6-access-group*

Syntax Description

ipv6-access-group	Name of the IPv6 access group. Names cannot contain a space or quotation mark, or begin with a numeric.

Command Default

No match criteria are configured.

Command Modes

Class-map configuration

Command History

Release	Modification
12.0(28)S	This command was introduced.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

For class-based weighted fair queueing (CBWFQ), you define traffic classes based on match criteria including access control lists (ACLs), protocols, input interfaces, QoS labels, and EXP field values. Packets satisfying the match criteria for a class constitute the traffic for that class.

The **match access-group name** command specifies an IPv6 named ACL only. The contents of the ACL are used as the match criteria against which packets are checked to determine if they belong to the class specified by the class map.

To use the **match access-group name** 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 dscp**
- **match mpls experimental**
- **match precedence**
- **match protocol**

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.

Examples

The following example specifies an access list named ipv6acl against whose contents packets will be checked to determine if they belong to the traffic class:

```
class-map ipv6_acl_class
match access-group name ipv6acl
```

Related Commands

Command	Description
match access-group	Configures the match criteria for a class map on the basis of the specified ACL.
match dscp	Identifies a specific IP DSCP value as a match criterion.
match mpls experimental	Configures a class map to use the specified value of the experimental (EXP) field as a match criterion.
match precedence	Identifies IP precedence values as match criteria.
match protocol	Configures the match criteria for a class map on the basis of the specified protocol.

match dscp

To identify one or more differentiated service code point (DSCP), Assured Forwarding (AF), and Certificate Server (CS) values as a match criterion, use the **match dscp** command in class-map configuration or policy inline configuration mode. To remove a specific DSCP value from a class map, use the **no** form of this command.

match [**ip**] **dscp** *dscp-value* [*dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value*]

no match [**ip**] **dscp** *dscp-value*

Syntax Description

ip	(Optional) Specifies that the match is for IPv4 packets only. If not used, the match is on both IPv4 and IPv6 packets. **Note** For the Cisco 10000 series routers, the **ip** keyword is required.
dscp-value	The DSCP value used to identify a DSCP value. For valid values, see the "Usage Guidelines."

Command Default

No match criteria are configured.
If you do not enter the **ip** keyword, matching occurs on both IPv4 and IPv6 packets.

Command Modes

Class-map configuration (config-cmap)
Policy inline configuration (config-if-spolicy-inline)

Command History

Release	Modification
12.2(13)T	This command was introduced. This command replaces the **match ip dscp** command.
12.0(28)S	This command was integrated into Cisco IOS Release 12.0(28)S for support in IPv6.
12.0(17)SL	This command was integrated into Cisco IOS Release 12.0(17)SL and implemented on the Cisco 10000 series routers.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 and introduced on Cisco ASR 1000 Series Routers.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T for Cisco Performance Monitor. Support was added for policy inline configuration mode.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE for Cisco Performance Monitor.

Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration mode in which you issue this command.

Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE

You must first enter the s**ervice-policy type performance-monitor inline** command.

DSCP Values

You must enter one or more differentiated service code point (DSCP) values. The command may include any combination of the following:

- Numbers (0 to 63) representing differentiated services code point values
- AF numbers (for example, af11) identifying specific AF DSCPs
- CS numbers (for example, cs1) identifying specific CS DSCPs
- **default**—Matches packets with the default DSCP.
- **ef**—Matches packets with EF DSCP.

For example, if you wanted the DCSP values of 0, 1, 2, 3, 4, 5, 6, or 7 (note that only one of the IP DSCP values must be a successful match criterion, not all of the specified DSCP values), enter the **match dscp 0 1 2 3 4 5 6 7** command.

This command is used by the class map to identify a specific DSCP value marking on a packet. In this context, *dscp-value* arguments are used as markings only and have no mathematical significance. For instance, the *dscp-value* of 2 is not greater than 1. The value simply indicates that a packet marked with the *dscp-value* of 2 is different than a packet marked with the *dscp-value* of 1. The treatment of these marked packets is defined by the user through the setting of Quality of Service (QoS) policies in policy-map class configuration mode.

Match Packets on DSCP Values

To match DSCP values for IPv6 packets only, the **match protocol ipv6** command must also be used. Without that command, the DSCP match defaults to match both IPv4 and IPv6 packets.

To match DSCP values for IPv4 packets only, use the **ip** keyword. Without the **ip** keyword the match occurs on both IPv4 and IPv6 packets. Alternatively, the **match protocol ip** command may be used with **match dscp** to classify only IPv4 packets.

After the DSCP bit is set, other QoS features can then operate on the bit settings.

The network can give priority (or some type of expedited handling) to marked traffic. Typically, you set the precedence value at the edge of the network (or administrative domain); data is then queued according to the precedence. Weighted fair queueing (WFQ) can speed up handling for high-precedence traffic at congestion points. Weighted Random Early Detection (WRED) can ensure that high-precedence traffic has lower loss rates than other traffic during times of congestion.

Cisco 10000 Series Routers

The Cisco 10000 series routers support DSCP matching of IPv4 packets only. You must include the **ip** keyword when specifying the DSCP values to use as match criterion.

You cannot use the **set ip dscp** command with the **set ip precedence** command to mark the same packet. DSCP and precedence values are mutually exclusive. A packet can have one value or the other, but not both.

Examples

The following example shows how to set multiple match criteria. In this case, two IP DSCP value and one AF value.

```
Router(config)# class-map map1
Router(config-cmap)# match dscp 1 2 af11
```

Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE

The following example shows how to use the policy inline configuration mode to configure a service policy for Performance Monitor. The policy specifies that packets traversing Ethernet interface 0/0 that match the criteria specified by DSCP value 2 will be monitored based on the parameters specified in the flow monitor configuration named **fm-2**:

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# match dscp 2
Router(config-if-spolicy-inline)# flow monitor fm-2
Router(config-if-spolicy-inline)# exit
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
service-policy type performance-monitor	Associates a Performance Monitor policy with an interface.
match protocol ip	Matches DSCP values for packets.
match protocol ipv6	Matches DSCP values for IPv6 packets.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
service-policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.
set dscp	Marks the DSCP value for packets within a traffic class.
show class-map	Displays all class maps and their matching criteria.

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 ipv6

To configure one or more of the IPv6 fields as a key field for a Flexible NetFlow flow record, use the **match ipv6** command in Flexible NetFlow flow record configuration mode. To disable the use of one or more of the IPv6 fields as a key field for a Flexible NetFlow flow record, use the **no** form of this command.

match ipv6 {**dscp** | **flow-label** | **next-header** | **payload-length** | **precedence** | **protocol** | **traffic-class** | **version**}

no match ipv6 {**dscp** | **flow-label** | **next-header** | **payload-length** | **precedence** | **protocol** | **traffic-class** | **version**}

Cisco Catalyst 6500 Switches in Cisco IOS Release 12.2(50)SY

match ipv6 {**dscp** | **precedence** | **protocol** | **tos**}

no match ipv6 {**dscp** | **precedence** | **protocol** | **tos**}

Syntax Description

dscp	Configures the IPv6 differentiated services code point DSCP (part of type of service (ToS)) as a key field.
flow-label	Configures the IPv6 flow label as a key field.
next-header	Configures the IPv6 next header as a key field.
payload-length	Configures the IPv6 payload length as a key field.
precedence	Configures the IPv6 precedence (part of ToS) as a key field.
protocol	Configures the IPv6 protocol as a key field.
tos	Configures the IPv6 ToS as a key field.
traffic-class	Configures the IPv6 traffic class as a key field.
version	Configures the IPv6 version from IPv6 header as a key field.

Command Default

The IPv6 fields are not configured as a key field.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7200 and Cisco 7300 Network Processing Engine (NPE) series routers.
12.2(50)SY	This command was modified. The **flow-label**, **next-header**, **payload-length**, **traffic-class** ,and **version** keywords were not supported in Cisco IOS Release 12.2(50)SY.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields differentiate flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

Note Some of the keywords of the **match ipv6** command are documented as separate commands. All of the keywords for the **match ipv6** command that are documented separately start with **match ipv6**. For example, for information about configuring the IPv6 hop limit as a key field for a Flexible NetFlow flow record, refer to the **match ipv6 hop-limit** command.

Examples

The following example configures the IPv6 DSCP field as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match ipv6 dscp
```

Related Commands

Command	Description
flow record	Creates a flow record.

match ipv6 access-list

To verify the sender's IPv6 address in inspected messages from the authorized prefix list, use the **match ipv6 access-list** command in router advertisement (RA) guard policy configuration mode.

match ipv6 access-list *ipv6-access-list-name*

Syntax Description

ipv6-access-list-name	Defines the IPv6 access list to be matched.

Command Default

Senders' IPv6 addresses are not verified.

Command Modes

RA guard policy configuration (config-ra-guard)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

The **match ipv6 access-list** command enables verification of the sender's IPv6 address in inspected messages from the configured authorized router source access list. If the **match ipv6 access-list** command is not configured, this authorization is bypassed.

An access list is configured using the **ipv6 access-list** command. For instance, to authorize the router with link-local address FE80::A8BB:CCFF:FE01:F700 only, define the following IPv6 access list:

```
Router(config)# ipv6 access-list list1
Router(config-ipv6-acl)# permit host FE80::A8BB:CCFF:FE01:F700 any
```

Examples

The following example defines an RA guard policy name as raguard1, places the router in RA guard policy configuration mode, and matches the IPv6 addresses in the access list named list1:

```
Router(config)# ipv6 nd raguard policy raguard1
Router(config-ra-guard)# match ipv6 access-list list1
```

Related Commands

Command	Description
ipv6 nd raguard policy	Defines the RA guard policy name and enter RA guard policy configuration mode.
ipv6 access-list	Defines an IPv6 access list and places the router in IPv6 access list configuration mode.

match ipv6 address

To distribute IPv6 routes that have a prefix permitted by a prefix list or to specify an IPv6 access list to use to match packets for policy-based routing (PBR) for IPv6, use the **match ipv6 address** command in route-map configuration mode. To remove the **match ipv6 address** entry, use the **no** form of this command.

match ipv6 address {**prefix-list** *prefix-list-name* | *access-list-name*}

no match ipv6 address

Syntax Description

prefix-list *prefix-list-name*	Specifies the name of an IPv6 prefix list.
access-list-name	Specifies the name of the IPv6 access list. Names cannot contain a space or quotation mark, or begin with a numeric.

Command Default

No routes are distributed based on destination network number.
No routes are distributed based on an access list.

Command Modes

Route-map configuration

Command History

Release	Modification
12.2(2)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 Release 12.2(14)S.
12.3(7)T	The *access-list-name* argument was added.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)S.
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.
12.2(33)SXI4	The **prefix-list** keyword and *prefix-list-name* argument are not supported in Cisco IOS Release 12.2(33)SXI4.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.

Usage Guidelines

Use the **route-map** command, and the **match** and **set** commands, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the match criteria—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met.

The **match ipv6 address** command can be used to specify either an access list or a prefix list. When using PBR, you must use the *access-list-name* argument—the **prefix-list** keyword and *prefix-list-name* argument will not work.

Examples

In the following example, IPv6 routes that have addresses specified by the prefix list named marketing are matched:

```
Router(config)# route-map name
Router(config-route-map)# match ipv6 address prefix-list marketing
```

In the following example, IPv6 routes that have addresses specified by an access list named marketing are matched:

```
Router(config-route-map)# match ipv6 address marketing
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community	Matches a BGP community.
match ipv6 address	Specifies an IPv6 access list to use to match packets for PBR for IPv6.
match ipv6 next-hop	Distributes IPv6 routes that have a next hop prefix permitted by a prefix list.
match ipv6 route-source	Distributes IPv6 routes that have been advertised by routers at an address specified by a prefix list.
match length	Bases policy routing on the Level 3 length of a packet.
match metric	Redistributes routes with the metric specified.
match route-type	Redistributes routes of the specified type.
route-map	Defines the conditions for redistributing routes from one routing protocol into another.
set as-path	Modifies an autonomous system path for BGP routes.
set community	Sets the BGP community attribute.
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Indicates where to output packets that pass a match clause of a route map for policy routing.
set ipv6 default next-hop	Specifies an IPv6 default next hop to which matching packets will be forwarded.
set ipv6 next-hop (PBR)	Indicates where to output IPv6 packets that pass a match clause of a route map for policy routing.
set ipv6 precedence	Sets the precedence value in the IPv6 packet header.
set level	Indicates where to import routes.
set local preference	Specifies a preference value for the autonomous system path.
set metric	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set tag	Sets a tag value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.

match ipv6 destination

To configure the IPv6 destination address as a key field for a Flexible NetFlow flow record, use the **match ipv6 destination** command in Flexible NetFlow flow record configuration mode. To disable the IPv6 destination address as a key field for a Flexible NetFlow flow record, use the **no** form of this command.

match ipv6 destination {**address** | {**mask** | **prefix**} [**minimum-mask** *mask*]}

no match ipv6 destination {**address** | {**mask** | **prefix**} [**minimum-mask** *mask*]}

Cisco Catalyst 6500 Switches in Cisco IOS Release 12.2(50)SY

match ipv6 destination address

no match ipv6 destination address

Syntax Description

address	Configures the IPv6 destination address as a key field.
mask	Configures the mask for the IPv6 destination address as a key field.
prefix	Configures the prefix for the IPv6 destination address as a key field.
minimum-mask *mask*	(Optional) Specifies the size, in bits, of the minimum mask. Range 1 to 128.

Command Default

The IPv6 destination address is not configured as a key field.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7200 and Cisco 7300 Network Processing Engine (NPE) series routers.
12.2(50)SY	This command was modified. The **mask**, **prefix**, and **minimum-mask** keywords were not supported in Cisco IOS Release 12.2(50)SY.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields differentiate flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

Examples

The following example configures a 16-bit IPv6 destination address prefix as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match ipv6 destination prefix minimum-mask 16
```

The following example specifies a 16-bit IPv6 destination address mask as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match ipv6 destination mask minimum-mask 16
```

Related Commands

Command	Description
flow record	Creates a flow record.

match ipv6 extension map

To configure the bitmap of the IPv6 extension header map as a key field for a Flexible NetFlow flow record, use the **match ipv6 extension map** command in Flexible NetFlow flow record configuration mode. To disable the use of the IPv6 bitmap of the IPv6 extension header map as a key field for a Flexible NetFlow flow record, use the **no** form of this command.

match ipv6 extension map

no match ipv6 extension map

Syntax Description

This command has no arguments or keywords.

Command Default

The use of the bitmap of the IPv6 extension header map as a key field for a user-defined Flexible NetFlow flow record is not enabled by default.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7200 and Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields differentiate flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

Bitmap of the IPv6 Extension Header Map

The bitmap of IPv6 extension header map is made up of 32 bits.

```
    0     1     2     3     4     5     6     7
+-----+-----+-----+-----+-----+-----+-----+-----+
| Res | FRA1| RH  | FRA0| UNK | Res | HOP | DST |
+-----+-----+-----+-----+-----+-----+-----+-----+
    8     9    10    11    12    13    14    15
+-----+-----+-----+-----+-----+-----+-----+-----+
| PAY | AH  | ESP |          Reserved           |
+-----+-----+-----+-----+-----+-----+-----+-----+
   16    17    18    19    20    21    22    23
+-----+-----+-----+-----+-----+-----+-----+-----+
|                  Reserved                     |
+-----+-----+-----+-----+-----+-----+-----+-----+
   24    25    26    27    28    29    30    31
+-----+-----+-----+-----+-----+-----+-----+-----+
|                  Reserved                     |
+-----+-----+-----+-----+-----+-----+-----+-----+
0  Res  Reserved
```

```
1  FRA1 Fragmentation header - not first fragment
2  RH   Routing header
3  FRA0 Fragment header - first fragment
4  UNK  Unknown Layer 4 header
        (compressed, encrypted, not supported)
5  Res  Reserved
6  HOP  Hop-by-hop option header
7  DST  Destination option header
8  PAY Payload compression header
9  AH  Authentication Header
10 ESP Encrypted security payload
11 to 31 Reserved
```

For more information on IPv6 headers, refer to RFC 2460 *Internet Protocol, Version 6 (IPv6)* at the following URL: http://www.ietf.org/rfc/rfc2460.txt.

Examples

The following example configures the IPv6 bitmap of the IPv6 extension header map of the packets in the flow as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match ipv6 extension map
```

Related Commands

Command	Description
flow record	Creates a flow record.

match ipv6 fragmentation

To configure one or more of the IPv6 fragmentation fields as a key field for a Flexible NetFlow flow record, use the **match ipv6 fragmentation** command in Flexible NetFlow flow record configuration mode. To disable the use of the IPv6 fragmentation field as a key field for a Flexible NetFlow flow record, use the **no** form of this command.

match IPv6 fragmentation {**flags** | **id** | **offset**}

no match IPv6 fragmentation {**flags** | **id** | **offset**}

Syntax Description

flags	Configures the IPv6 fragmentation flags as a key field.
id	Configures the IPv6 fragmentation ID as a key field.
offset	Configures the IPv6 fragmentation offset value as a key field.

Command Default

The IPv6 fragmentation field is not configured as a key field.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7200 and Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields differentiate flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

Examples

The following example configures the IPv6 fragmentation flags a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match ipv6 fragmentation flags
```

The following example configures the IPv6 offset value a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match ipv6 fragmentation offset
```

Related Commands

Command	Description
flow record	Creates a flow record.

match ipv6 hop-limit

To configure the IPv6 hop limit as a key field for a Flexible NetFlow flow record, use the **match ipv6 hop-limit** command in Flexible NetFlow flow record configuration mode. To disable the use of a section of an IPv6 packet as a key field for a Flexible NetFlow flow record, use the **no** form of this command.

match ipv6 hop-limit

no match ipv6 hop-limit

Syntax Description

This command has no arguments or keywords.

Command Default

The use of the IPv6 hop limit as a key field for a user-defined Flexible NetFlow flow record is not enabled by default.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7200 and Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields differentiate flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

Examples

The following example configures the hop limit of the packets in the flow as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match ipv6 hop-limit
```

Related Commands

Command	Description
flow record	Creates a flow record.

match ipv6 length

To configure one or more of the IPv6 length fields as a key field for a Flexible NetFlow flow record, use the **match ipv6 length** command in Flexible NetFlow flow record configuration mode. To disable the use of the IPv6 length field as a key field for a Flexible NetFlow flow record, use the **no** form of this command.

match ipv6 length {**header** | **payload** | **total**}

no match ipv6 length {**header** | **payload** | **total**}

Syntax Description

header	Configures the length in bytes of the IPv6 header, not including any extension headers as a key field.
payload	Configures the length in bytes of the IPv6 payload, including any extension header as a key field.
total	Configures the total length in bytes of the IPv6 header and payload as a key field.

Command Default

The IPv6 length field is not configured as a key field.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7200 and Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields differentiate flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

Examples

The following example configures the length of the IPv6 header in bytes, not including any extension headers, as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match ipv6 length header
```

Related Commands

Command	Description
flow record	Creates a flow record.

match ipv6 next-hop

To distribute IPv6 routes that have a next hop prefix permitted by a prefix list, use the **match ipv6 next-hop** command in route-map configuration mode. To remove the **match ipv6 next-hop** entry, use the **no** form of this command.

match ipv6 next-hop prefix-list *prefix-list-name*

no match ipv6 next-hop

Syntax Description

prefix-list *prefix-list-name*	Name of an IPv6 prefix list.

Command Default

Routes are distributed freely, without being required to match a next hop address.

Command Modes

Route-map configuration

Command History

Release	Modification
12.2(2)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 Release 12.2(14)S.
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.
12.2(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 **match ipv6 next-hop** command is similar to the **match ip next-hop** command, except that it is IPv6-specific.

Use the **route-map** command, and the **match** and **set** commands, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the *set actions*—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **match** command has multiple formats. The **match** commands can be given in any order, and all **match** commands must "pass" to cause the route to be redistributed according to the *set actions* given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

When you are passing routes through a route map, a route map can have several parts. Any route that does not match at least one **match** command relating to a **route-map** command will be ignored; that is, the route will not be advertised for outbound route maps and will not be accepted for inbound route maps. If you want to modify only some data, you must configure a second route map section with an explicit match specified.

Note A permit route map containing only **set** commands and no **match** commands permits all routes.

Examples

The following example distributes routes that have a next hop IPv6 address passed by the prefix list named marketing:

```
Router(config)# route-map name
Router(config-route-map)# match ipv6 next-hop prefix-list marketing
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community	Matches a BGP community.
match ipv6 address	Distributes IPv6 routes that have a prefix permitted by a prefix list.
match ipv6 route-source	Distributes IPv6 routes that have been advertised by routers at an address specified by a prefix list.
match metric	Redistributes routes with the metric specified.
match route-type	Redistributes routes of the specified type.
route-map	Defines the conditions for redistributing routes from one routing protocol into another.
set as-path	Modifies an autonomous system path for BGP routes.
set community	Sets the BGP community attribute.
set level	Indicates where to import routes.
set local preference	Specifies a preference value for the autonomous system path.
set metric	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set tag	Sets a tag value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.

match ipv6 route-source

To distribute IPv6 routes that have been advertised by routers at an address specified by a prefix list, use the **match ipv6 route-source** command in route-map configuration mode. To remove the **match ipv6 route-source** entry, use the **no** form of this command.

match ipv6 route-source prefix-list *prefix-list-name*

no match ipv6 route-source

Syntax Description

prefix-list *prefix-list-name*	Name of an IPv6 prefix list.

Command Default

No filtering on route source.

Command Modes

Route-map configuration

Command History

Release	Modification
12.2(2)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 Release 12.2(14)S.
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.
12.2(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 **match ipv6 route-source** command is similar to the **match ip route-source** command, except that it is IPv6-specific.

Use the **route-map** command, and the **match** and **set** commands, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the *set actions*—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **match** command has multiple formats. The **match** commands can be given in any order, and all **match** commands must "pass" to cause the route to be redistributed according to the *set actions* given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

When you are passing routes through a route map, a route map can have several parts. Any route that does not match at least one **match** command relating to a **route-map** command will be ignored; that is, the route will not be advertised for outbound route maps and will not be accepted for inbound route maps. If you want to modify only some data, you must configure a second route map section with an explicit match specified.

There are situations in which the next hop for a route and the source networking device address are not the same.

Note A permit route map containing only **set** commands and no **match** commands permits all routes.

Examples

The following example distributes routes that have been advertised by networking devices at the addresses specified by the prefix list named marketing:

```
Router(config)# route-map name
Router(config-route-map)# match ipv6 route-source prefix-list marketing
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community	Matches a BGP community.
match ipv6 address	Distributes IPv6 routes that have a prefix permitted by a prefix list.
match ipv6 next-hop	Distributes IPv6 routes that have a next hop prefix permitted by a prefix list.
match metric	Redistributes routes with the metric specified.
match route-type	Redistributes routes of the specified type.
route-map	Defines the conditions for redistributing routes from one routing protocol into another.
set as-path	Modifies an autonomous system path for BGP routes.
set community	Sets the BGP community attribute.
set level	Indicates where to import routes.
set local preference	Specifies a preference value for the autonomous system path.
set metric	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set tag	Sets a tag value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.

match length

To base policy routing on the Level 3 length of a packet, use the **match length** command in route-map configuration mode. To remove the entry, use the **no** form of this command.

match length *minimum-length maximum-length*

no match length *minimum-length maximum-length*

Syntax Description

minimum-length	Minimum Level 3 length of the packet, inclusive, allowed for a match. Range is from 0 to 0x7FFFFFFF.
maximum-length	Maximum Level 3 length of the packet, inclusive, allowed for a match. Range is from 0 to 0x7FFFFFFF.

Command Default

No policy routing occurs on the length of a packet.

Command Modes

Route-map configuration

Command History

Release	Modification
10.0	This command was introduced.
12.3(7)T	This command was updated for use in configuring IPv6 policy-based routing (PBR).
12.2SX	This command is supported in the Cisco 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 modified. It was integrated into Cisco IOS XE Release 3.2S.

Usage Guidelines

In IPv4, use the **ip policy route-map** interface configuration command, the **route-map** global configuration command, and the **match** and **set** route-map configuration commands, to define the conditions for policy routing packets. The **ip policy route-map** command identifies a route map by name. Each **route-map** has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*—the conditions under which policy routing occurs. The **set** commands specify the *set actions*—the particular routing actions to perform if the criteria enforced by the **match** commands are met.

In PBR for IPv6, use the **ipv6 policy route-map** or **ipv6 local policy route-map** command to define conditions for policy routing packets.

In IPv4, the **match** route-map configuration command has multiple formats. The **match** commands can be given in any order, and all **match** commands must "pass" to cause the packet to be routed according to the *set actions* given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

In IPv4, you might want to base your policy routing on the length of packets so that your interactive traffic and bulk traffic are directed to different routers.

Examples

In the following example, packets 3 to 200 bytes long, inclusive, will be routed to FDDI interface 0:

```
interface serial 0
 ip policy route-map interactive
!
route-map interactive
 match length 3 200
 set interface fddi 0
```

In the following example for IPv6, packets 3 to 200 bytes long, inclusive, will be routed to FDDI interface 0:

```
interface Ethernet0/0
  ipv6 policy-route-map interactive
!
route-map interactive
 match length 3 200
 set interface fddi 0
```

Related Commands

Command	Description
ip local policy route-map	Identifies a route map to use for policy routing on an interface.
ipv6 local policy route-map	Configures PBR for IPv6 for originated packets.
ipv6 policy route-map	Configures IPv6 PBR on an interface.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match ipv6 address	Specifies an IPv6 access list to use to match packets for PBR for IPv6.
match length	Bases policy routing on the Level 3 length of a packet.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Indicates where to output packets that pass a match clause of route map for policy routing.
set ip default next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing and for which the Cisco IOS software has no explicit route to a destination.
set ipv6 default next-hop	Specifies an IPv6 default next hop to which matching packets will be forwarded.
set ip next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing.

Command	Description
set ipv6 next-hop (PBR)	Indicates where to output IPv6 packets that pass a match clause of a route map for policy routing.
set ipv6 precedence	Sets the precedence value in the IPv6 packet header.

match mpls-label

To redistribute routes that include Multiprotocol Label Switching (MPLS) labels if the routes meet the conditions specified in the route map, use the **match mpls-label** command in route-map configuration mode. To disable this function, use the **no** form of this command.

match mpls-label

no match mpls-label

Syntax Description

This command has no arguments or keywords.

Command Default

Routes with MPLS labels are not redistributed.

Command Modes

Route-map configuration

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(11)S	This command was integrated into Cisco IOS Release 12.2(11)S.
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.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

A route map that includes this command can be used in the following instances:

- With the **neighbor route-map in** command to manage inbound route maps in BGP
- With the **redistribute bgp** command to redistribute route maps in an IGP

Use the **route-map** global configuration command, and the **match** and **set** route map configuration commands, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the match criteria—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **match route-map** configuration command has multiple formats. The **match** commands can be given in any order, and all **match** commands must "pass" to cause the route to be redistributed according to the set actions given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

When you are passing routes through a route map, a route map can have several parts. Any route that does not match at least one match clause relating to a **route-map** command will be ignored; that is, the route will not be advertised for outbound route maps and will not be accepted for inbound route maps. If you want to modify only some data, you must configure a second route map section with an explicit match specified.

Examples

The following example shows how to create a route map that redistributes routes if the following conditions are met:

- The IP address of the route matches an IP address in access control list 2.
- The route includes an MPLS label.

```
Router(config-router)# route-map incoming permit 10
Router(config-route-map)# match ip address 2
Router(config-route-map)# match mpls-label
```

Related Commands

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.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set mpls-label	Enables a route to be distributed with an MPLS label if the route matches the conditions specified in the route map.

match precedence

To identify IP precedence values to use as the match criterion, use the **match precedence** command in class-map configuration or policy inline configuration mode. To remove IP precedence values from a class map, use the **no** form of this command.

match [**ip**] **precedence** {*precedence-criteria1* | *precedence-criteria2* | *precedence-criteria3* | *precedence-criteria4*}

no match [**ip**] **precedence** {*precedence-criteria1* | *precedence-criteria2* | *precedence-criteria3* | *precedence-criteria4*}

Syntax Description

ip	(Optional) Specifies that the match is for IPv4 packets only. If not used, the match is on both IP and IPv6 packets. **Note** For the Cisco 10000 series routers, the **ip** keyword is required.
precedence-criteria1 *precedence-criteria2* *precedence-criteria3* *precedence-criteria4*	Identifies the precedence value. You can enter up to four different values, separated by a space. See the "Usage Guidelines" for valid values.

Command Default

No match criterion is configured.
If you do not enter the **ip** keyword, matching occurs on both IPv4 and IPv6 packets.

Command Modes

Class-map configuration (config-cmap)
Policy inline configuration (config-if-spolicy-inline)

Command History

Release	Modification
12.2(13)T	This command was introduced. This command replaces the **match ip precedence** command.
12.0(17)SL	This command was integrated into Cisco IOS Release 12.0(17)SL and implemented on the Cisco 10000 series routers.
12.0(28)S	This command was integrated into Cisco IOS Release 12.0(28)S for IPv6.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T for Cisco Performance Monitor. Support was added for policy inline configuration mode.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE for Cisco Performance Monitor.

Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration mode in which you issue this command.

You can enter up to four matching criteria, as number abbreviation (0 to 7) or criteria names (critical, flash, and so on), in a single match statement. For example, if you wanted the precedence values of 0, 1, 2, or 3 (note that only one of the precedence values must be a successful match criterion, not all of the specified precedence values), enter the **match ip precedence 0 1 2 3** command. The *precedence-criteria* numbers are not mathematically significant; that is, the *precedence-criteria* of 2 is not greater than 1. The way that these different packets are treated depends upon quality of service (QoS) policies, set in the policy-map configuration mode.

You can configure a QoS policy to include IP precedence marking for packets entering the network. Devices within your network can then use the newly marked IP precedence values to determine how to treat the packets. For example, class-based weighted random early detection (WRED) uses IP precedence values to determine the probability that a packet is dropped. You can also mark voice packets with a particular precedence. You can then configure low-latency queueing (LLQ) to place all packets of that precedence into the priority queue.

Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE

You must first enter the s**ervice-policy type performance-monitor inline** command.

Matching Precedence for IPv6 and IPv4 Packets on the Cisco 10000 and 7600 Series Routers

On the Cisco 7600 series and 10000 series routers, you set matching criteria based on precedence values for only IPv6 packets using the **match protocol** command with the **ipv6** keyword. Without that keyword, the precedence match defaults to match both IPv4 and IPv6 packets. You set matching criteria based on precedence values for IPv4 packets only, use the **ip** keyword. Without the **ip** keyword the match occurs on both IPv4 and IPv6 packets.

Precedence Values and Names

The following table lists all criteria conditions by value, name, binary value, and recommended use. You may enter up to four criteria, each separated by a space. Only one of the precedence values must be a successful match criterion. Table 34 lists the IP precedence values.

Table 34 IP Precedence Values

Precedence Value	Precedence Name	Binary Value	Recommended Use
0	routine	000	Default marking value
1	priority	001	Data applications
2	immediate	010	Data applications
3	flash	011	Call signaling
4	flash-override	100	Video conferencing and streaming video
5	critical	101	Voice
6	internet (control)	110	Network control traffic (such as routing, which is typically precedence 6)
7	network (control)	111	

Do not use IP precedence 6 or 7 to mark packets, unless you are marking control packets.

Examples

IPv4-Specific Traffic Match

The following example shows how to configure the service policy named priority50 and attach service policy priority50 to an interface, matching for IPv4 traffic only. In a network where both IPv4 and IPv6 are running, you might find it necessary to distinguish between the protocols for matching and traffic segregation. In this example, the class map named ipprec5 will evaluate all IPv4 packets entering Fast Ethernet interface 1/0/0 for a precedence value of 5. If the incoming IPv4 packet has been marked with the precedence value of 5, the packet will be treated as priority traffic and will be allocated with bandwidth of 50 kbps.

```
Router(config)# class-map ipprec5
Router(config-cmap)# match ip precedence 5
Router(config)# exit
Router(config)# policy-map priority50
Router(config-pmap)# class ipprec5
Router(config-pmap-c)# priority 50
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fa1/0/0
Router(config-if)# service-policy input priority50
```

IPv6-Specific Traffic Match

The following example shows the same service policy matching on precedence for IPv6 traffic only. Notice that the **match protocol** command with the **ipv6** keyword precedes the **match precedence** command. The **match protocol** command is required to perform matches on IPv6 traffic alone.

```
Router(config)# class-map ipprec5
Router(config-cmap)# match protocol ipv6
Router(config-cmap)# match precedence 5
Router(config)# exit
Router(config)# policy-map priority50
Router(config-pmap)# class ipprec5
Router(config-pmap-c)# priority 50
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fa1/0/0
Router(config-if)# service-policy input priority50
```

Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE

The following example shows how to use the policy inline configuration mode to configure a service policy for Performance Monitor. The policy specifies that packets traversing Ethernet interface 0/0 that match the criteria of a match precedence of 4 will be monitored based on the parameters specified in the flow monitor configuration named **fm-2**:

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# match precedence 4
Router(config-if-spolicy-inline)# flow monitor fm-2
Router(config-if-spolicy-inline)# exit
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
service-policy type performance-monitor	Associates a Performance Monitor policy with an interface.
match protocol	Configures the match criteria for a class map on the basis of a specified protocol.

Command	Description
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
service-policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.
set ip precedence	Sets the precedence value in the IP header.
show class-map	Displays all class maps and their matching criteria, or a specified class map and its matching criteria.

match protocol

To configure the match criterion for a class map on the basis of a specified protocol, use the **match protocol** command in class-map configuration or policy inline configuration mode. To remove the protocol-based match criterion from the class map, use the **no** form of this command.

match protocol *protocol-name*

no match protocol *protocol-name*

Syntax Description

protocol-name	Name of the protocol (for example, bgp) used as a matching criterion. See the "Usage Guidelines" for a list of protocols supported by most routers.

Command Default

No match criterion is configured.

Command Modes

Class-map configuration (config-cmap)
Policy inline configuration (config-if-spolicy-inline)

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.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.1(13)E	This command was integrated into Cisco IOS Release 12.1(13)E and implemented on Catalyst 6000 family switches without FlexWAN modules.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(13)T	This command was modified to remove **apollo**, **vines**, and **xns** from the list of protocols used as matching criteria. These protocols were removed because Apollo Domain, Banyan VINES, and Xerox Network Systems (XNS) were removed in this release. The IPv6 protocol was added to support matching on IPv6 packets.
12.0(28)S	This command was integrated into Cisco IOS Release 12.0(28)S for IPv6.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(17a)SX1	This command was integrated into Cisco IOS Release 12.2(17a)SX1.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE and implemented on the Supervisor Engine 720.
12.4(6)T	This command was modified. The Napster protocol was removed because it is no longer supported.
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 and implemented on the Cisco 10000 series routers.

Release	Modification
12.2(18)ZY	This command was integrated into Cisco IOS Release 12.2(18)ZY. This command was modified to enhance Network-Based Application Recognition (NBAR) functionality on the Catalyst 6500 series switch that is equipped with the Supervisor 32/programmable intelligent services accelerator (PISA) engine.
12.4(15)XZ	This command was integrated into Cisco IOS Release 12.4(15)XZ.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T and implemented on the Cisco 1700, Cisco 1800, Cisco 2600, Cisco 2800, Cisco 3700, Cisco 3800, Cisco 7200, and Cisco 7300 series routers.
Cisco IOS XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2 and implemented on the Cisco ASR 1000 Series Routers.
Cisco IOS XE Release 3.1S	This command was modified. Support for more protocols was added.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T for Cisco Performance Monitor. Support was added for policy inline configuration mode.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE for Cisco Performance Monitor.

Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration mode in which you issue this command.

Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE

You must first enter the s**ervice-policy type performance-monitor inline** command.

Supported Platforms Other Than Cisco 7600 Routers and Cisco 10000 Series Routers

For class-based weighted fair queueing (CBWFQ), you define traffic classes based on match criteria protocols, access control lists (ACLs), input interfaces, quality of service (QoS) labels, and Experimental (EXP) field values. Packets satisfying the match criteria for a class constitute the traffic for that class.

The **match protocol** command specifies the name of a protocol to be used as the match criteria against which packets are checked to determine if they belong to the class specified by the class map.

The **match protocol ipx** command matches packets in the output direction only.

To use the **match protocol** 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**

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.

To configure NBAR to match protocol types that are supported by NBAR traffic, use the **match protocol** (NBAR) command.

Cisco 7600 Series Routers

The **match protocol** command in QoS class-map configuration configures NBAR and sends all traffic on the port, both ingress and egress, to be processed in the software on the Multilayer Switch Feature Card 2 (MSFC2).

For CBWFQ, you define traffic classes based on match criteria like protocols, ACLs, input interfaces, QoS labels, and Multiprotocol Label Switching (MPLS) EXP field values. Packets satisfying the match criteria for a class constitute the traffic for that class.

The **match protocol** command specifies the name of a protocol to be used as the match criteria against which packets are checked to determine if they belong to the class specified by the class map.

If you want to use the **match protocol** command, you must first enter the **class-map** command to specify the name of the class to which you want to establish the match criteria.

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.

This command can be used to match protocols that are known to the NBAR feature. For a list of protocols supported by NBAR, see the "Classification" part of the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Cisco 10000 Series Routers

For CBWFQ, you define traffic classes based on match criteria including protocols, ACLs, input interfaces, QoS labels, and EXP field values. Packets satisfying the match criteria for a class constitute the traffic for that class.

The **match protocol** command specifies the name of a protocol to be used as the match criteria against which packets are checked to determine if they belong to the class specified by the class map.

The **match protocol ipx** command matches packets in the output direction only.

To use the **match protocol** command, you must first enter the **class-map** command to specify the name of the class whose match criteria you want to establish.

If you are matching NBAR protocols, use the **match protocol** (NBAR) command.

Match Protocol Command Restrictions (Catalyst 6500 Series Switches Only)

Policy maps contain traffic classes. Traffic classes contain one or more **match** commands that can be used to match packets (and organize them into groups) on the basis of a protocol type or application. You can create as many traffic classes as needed.

Cisco IOS Release 12.2(18)ZY includes software intended for use on the Catalyst 6500 series switch that is equipped with a Supervisor 32/PISA engine. For this release and platform, note the following restrictions for using policy maps and **match protocol** commands:

- A single traffic class can be configured to match a maximum of 8 protocols or applications.
- Multiple traffic classes can be configured to match a cumulative maximum of 95 protocols or applications.

Supported Protocols

Table 35 lists the protocols supported by most routers. Some routers support a few additional protocols. For example, the Cisco 7600 router supports the AARP and DECnet protocols, while the Cisco 7200 router supports the directconnect and PPPOE protocols. For a complete list of supported protocols, see the online help for the **match protocol** command on the router that you are using.

Table 35 Supported Protocols

Protocol Name	Description
802-11-iapp	IEEE 802.11 Wireless Local Area Networks Working Group Internet Access Point Protocol
ace-svr	ACE Server/Propagation
aol	America-Online Instant Messenger
appleqtc	Apple QuickTime
arp*	IP Address Resolution Protocol (ARP)
bgp	Border Gateway Protocol
biff	Biff mail notification
bootpc	Bootstrap Protocol Client
bootps	Bootstrap Protocol Server
bridge*	bridging
cddbp	CD Database Protocol
cdp*	Cisco Discovery Protocol
cifs	CIFS
cisco-fna	Cisco FNATIVE
cisco-net-mgmt	cisco-net-mgmt
cisco-svcs	Cisco license/perf/GDP/X.25/ident svcs
cisco-sys	Cisco SYSMAINT
cisco-tdp	cisco-tdp
cisco-tna	Cisco TNATIVE
citrix	Citrix Systems Metaframe
citriximaclient	Citrix IMA Client
clns*	ISO Connectionless Network Service
clns_es*	ISO CLNS End System
clns_is*	ISO CLNS Intermediate System
clp	Cisco Line Protocol
cmns*	ISO Connection-Mode Network Service
cmp	Cluster Membership Protocol
compressedtcp*	Compressed TCP
creativepartnr	Creative Partner
creativeserver	Creative Server
cuseeme	CU-SeeMe desktop video conference
daytime	Daytime (RFC 867)
dbase	dBASE Unix
dbcontrol_agent	Oracle Database Control Agent
ddns-v3	Dynamic DNS Version 3

Table 35 Supported Protocols (continued)

Protocol Name	Description
dhcp	Dynamic Host Configuration
dhcp-failover	DHCP Failover
directconnect	Direct Connect
discard	Discard port
dns	Domain Name Server lookup
dnsix	DNSIX Security Attribute Token Map
echo	Echo port
edonkey	eDonkey
egp	Exterior Gateway Protocol
eigrp	Enhanced Interior Gateway Routing Protocol
entrust-svc-handler	Entrust KM/Admin Service Handler
entrust-svcs	Entrust sps/aaas/aams
exec	Remote Process Execution
exchange	Microsoft RPC for Exchange
fasttrack	FastTrack Traffic (KaZaA, Morpheus, Grokster, and so on)
fcip-port	FCIP
finger	Finger
ftp	File Transfer Protocol
ftps	FTP over TLS/SSL
gdoi	Group Domain of Interpretation
giop	Oracle GIOP/SSL
gnutella	Gnutella Version 2 Traffic (BearShare, Shareeza, Morpheus, and so on)
gopher	Gopher
gre	Generic Routing Encapsulation
gtpv0	GPRS Tunneling Protocol Version 0
gtpv1	GPRS Tunneling Protocol Version 1
h225ras	H225 RAS over Unicast
h323	H323 Protocol
h323callsigalt	H323 Call Signal Alternate
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	Hypertext Transfer Protocol
https	Secure Hypertext Transfer Protocol
ica	ica (Citrix)

Table 35 Supported Protocols (continued)

Protocol Name	Description
icabrowser	icabrowser (Citrix)
icmp	Internet Control Message Protocol
ident	Authentication Service
igmpv3lite	IGMP over UDP for SSM
imap	Internet Message Access Protocol
imap3	Interactive Mail Access Protocol 3
imaps	IMAP over TLS/SSL
ip*	IP (version 4)
ipass	IPASS
ipinip	IP in IP (encapsulation)
ipsec	IP Security Protocol (ESP/AH)
ipsec-msft	Microsoft IPsec NAT-T
ipv6*	IP (version 6)
ipx	IPX
irc	Internet Relay Chat
irc-serv	IRC-SERV
ircs	IRC over TLS/SSL
ircu	IRCU
isakmp	ISAKMP
iscsi	iSCSI
iscsi-target	iSCSI port
kazaa2	Kazaa Version 2
kerberos	Kerberos
l2tp	Layer 2 Tunnel Protocol
ldap	Lightweight Directory Access Protocol
ldap-admin	LDAP admin server port
ldaps	LDAP over TLS/SSL
llc2*	llc2
login	Remote login
lotusmtap	Lotus Mail Tracking Agent Protocol
lotusnote	Lotus Notes
mgcp	Media Gateway Control Protocol
microsoft-ds	Microsoft-DS
msexch-routing	Microsoft Exchange Routing
msnmsgr	MSN Instant Messenger
msrpc	Microsoft Remote Procedure Call

Table 35 Supported Protocols (continued)

Protocol Name	Description
msrpc-smb-netbios	MSRPC over TCP port 445
ms-cluster-net	MS Cluster Net
ms-dotnetster	Microsoft .NETster Port
ms-sna	Microsoft SNA Server/Base
ms-sql	Microsoft SQL
ms-sql-m	Microsoft SQL Monitor
mysql	MySQL
n2h2server	N2H2 Filter Service Port
ncp	NCP (Novell)
net8-cman	Oracle Net8 Cman/Admin
netbios	Network Basic Input/Output System
netbios-dgm	NETBIOS Datagram Service
netbios-ns	NETBIOS Name Service
netbios-ssn	NETBIOS Session Service
netshow	Microsoft Netshow
netstat	Variant of systat
nfs	Network File System
nntp	Network News Transfer Protocol
novadigm	Novadigm Enterprise Desktop Manager (EDM)
ntp	Network Time Protocol
oem-agent	OEM Agent (Oracle)
oracle	Oracle
oracle-em-vp	Oracle EM/VP
oraclenames	Oracle Names
orasrv	Oracle SQL*Net v1/v2
ospf	Open Shortest Path First
pad*	Packet assembler/disassembler (PAD) links
pcanywhere	Symantec pcANYWHERE
pcanywheredata	pcANYWHEREdata
pcanywherestat	pcANYWHEREstat
pop3	Post Office Protocol
pop3s	POP3 over TLS/SSL
pppoe	Point-to-Point Protocol over Ethernet
pptp	Point-to-Point Tunneling Protocol
printer	Print spooler/ldp
pwdgen	Password Generator Protocol

Table 35 Supported Protocols (continued)

Protocol Name	Description
qmtp	Quick Mail Transfer Protocol
radius	RADIUS & Accounting
rcmd	Berkeley Software Distribution (BSD) r-commands (rsh, rlogin, rexec)
rdb-dbs-disp	Oracle RDB
realmedia	RealNetwork's Realmedia Protocol
realsecure	ISS Real Secure Console Service Port
rip	Routing Information Protocol
router	Local Routing Process
rsrb*	Remote Source-Route Bridging
rsvd	RSVD
rsvp	Resource Reservation Protocol
rsvp-encap	RSVP ENCAPSULATION-1/2
rsvp_tunnel	RSVP Tunnel
rtc-pm-port	Oracle RTC-PM port
rtelnet	Remote Telnet Service
rtp	Real-Time Protocol
rtsp	Real-Time Streaming Protocol
r-winsock	remote-winsock
secure-ftp	FTP over Transport Layer Security/Secure Sockets Layer (TLS/SSL)
secure-http	Secured HTTP
secure-imap	Internet Message Access Protocol over TLS/SSL
secure-irc	Internet Relay Chat over TLS/SSL
secure-ldap	Lightweight Directory Access Protocol over TLS/SSL
secure-nntp	Network News Transfer Protocol over TLS/SSL
secure-pop3	Post Office Protocol over TLS/SSL
secure-telnet	Telnet over TLS/SSL
send	SEND
shell	Remote command
sip	Session Initiation Protocol
sip-tls	Session Initiation Protocol-Transport Layer Security
skinny	Skinny Client Control Protocol
sms	SMS RCINFO/XFER/CHAT
smtp	Simple Mail Transfer Protocol
snapshot	Snapshot routing support
snmp	Simple Network Protocol
snmptrap	SNMP Trap

Table 35 Supported Protocols (continued)

Protocol Name	Description
socks	Sockets network proxy protocol (SOCKS)
sqlnet	Structured Query Language (SQL)*NET for Oracle
sqlserv	SQL Services
sqlsrv	SQL Service
sqlserver	Microsoft SQL Server
ssh	Secure shell
sshell	SSLshell
ssp	State Sync Protocol
streamwork	Xing Technology StreamWorks player
stun	cisco Serial Tunnel
sunrpc	Sun remote-procedure call (RPC)
syslog	System Logging Utility
syslog-conn	Reliable Syslog Service
tacacs	Login Host Protocol (TACACS)
tacacs-ds	TACACS-Database Service
tarantella	Tarantella
tcp	Transport Control Protocol
telnet	Telnet
telnets	Telnet over TLS/SSL
tftp	Trivial File Transfer Protocol
time	Time
timed	Time server
tr-rsrb	cisco RSRB
tto	Oracle TTC/SSL
udp	User Datagram Protocol
uucp	UUCPD/UUCP-RLOGIN
vdolive	VDOLive streaming video
vofr*	Voice over Frame Relay
vqp	VLAN Query Protocol
webster	Network Dictionary
who	Who's service
wins	Microsoft WINS
x11	X Window System
xdmcp	XDM Control Protocol
xwindows*	X-Windows remote access
ymsgr	Yahoo! Instant Messenger

* This protocol is not supported on the Catalyst 6500 series switch that is equipped with a Supervisor 32/PISA engine.

Examples

The following example specifies a class map named ftp and configures the FTP protocol as a match criterion:

```
Router(config)# class-map ftp
Router(config-cmap)# match protocol ftp
```

Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE

The following example shows how to use the policy inline configuration mode to configure a service policy for Performance Monitor. The policy specifies that packets traversing Ethernet interface 0/0 for the IP protocol will be monitored based on the parameters specified in the flow monitor configuration named **fm-2**:

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# match protocol ip
Router(config-if-spolicy-inline)# flow monitor fm-2
Router(config-if-spolicy-inline)# exit
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
service-policy type performance-monitor	Associates a Performance Monitor policy with an interface.
match access-group	Configures the match criteria for a class map based on the specified ACL.
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 value of the experimental field as a match criterion.
match precedence	Identifies IP precedence values as match criteria.
match protocol (NBAR)	Configures NBAR to match traffic by a protocol type known to NBAR.
match qos-group	Configures a class map to use the specified EXP field value as a match criterion.

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 ra prefix-list

To verify the advertised prefixes in inspected messages from the authorized prefix list, use the **match ra prefix-list** command in router advertisement (RA) guard policy configuration mode.

match ra prefix-list *ipv6-prefix-list-name*

Syntax Description

ipv6-prefix-list-name	Defines the IPv6 prefix list to be matched.

Command Default

Advertised prefixes are not verified.

Command Modes

RA guard policy configuration (config-ra-guard)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

The **match ra prefix-list** command enables verification of the advertised prefixes in inspected messages from the configured authorized prefix list. Use the **ipv6 prefix-list** command to configure an IPv6 prefix list. For instance, to authorize the 2001:100::/64 prefixes and deny the 2002:100::/64 prefixes, define the following IPv6 prefix list:

```
Router(config)# ipv6 prefix-list listname1 deny 2001:0DB8:101:/64
Router(config)# ipv6 prefix-list listname1 permit 2001:0DB8:100::/64
```

Examples

The following example defines an RA guard policy name as raguard1, places the router in RA guard policy configuration mode, and verifies the advertised prefixes in listname1:

```
Router(config)# ipv6 nd raguard policy raguard1
Router(config-ra-guard)# match ra prefix-list listname1
```

Related Commands

Command	Description
ipv6 nd raguard policy	Defines the RA guard policy name and enter RA guard policy configuration mode.
ipv6 prefix-list	Creates an entry in an IPv6 prefix list.

max-metric router-lsa

To configure a router that is running the Open Shortest Path First (OSPF) protocol to advertise a maximum metric so that other routers do not prefer the router as an intermediate hop in their shortest path first (SPF) calculations, use the **max-metric router-lsa** command in router address family topology or router configuration mode. To disable the advertisement of a maximum metric, use the **no** form of this command.

max-metric router-lsa [**external-lsa** [*max-metric-value*]] [**include-stub**] [**inter-area-lsas** [*max-metric-value*]] [**on-startup** {*seconds* | **wait-for-bgp**}] [**prefix-lsa**] [**stub-prefix-lsa** [*max-metric-value*]] [**summary-lsa** [*max-metric-value*]]

no max-metric router-lsa [**external-lsa** [*max-metric-value*]] [**include-stub**] [**inter-area-lsas** [*max-metric-value*]] [**on-startup** {*seconds* | **wait-for-bgp**}] [**prefix-lsa**] [**stub-prefix-lsa** [*max-metric-value*]] [**summary-lsa** [*max-metric-value*]]

Syntax Description

external-lsa	(Optional) Configures the router to override the external LSA metric with the maximum metric value.
max-metric-value	(Optional) Maximum metric value for LSAs. The configurable range is from 1 to 16777215. The default value is 16711680.
include-stub	(Optional) Configures the router to advertise the maximum metric for stub links in router LSAs.
inter-area-lsas	(Optional) Configures the router to override the inter-area LSA metric with the maximum metric value.
on-startup	(Optional) Configures the router to advertise a maximum metric at startup.
seconds	(Optional) Maximum metric value for the specified time interval. The configurable range is from 5 to 86400 seconds. There is no default timer value for this configuration option.
wait-for-bgp	(Optional) Configures the router to advertise a maximum metric until Border Gateway Protocol (BGP) routing tables have converged or the default timer has expired. The default timer is 600 seconds.
prefix-lsa	(Optional) Configures the router to advertise the maximum metric for prefix links in router LSAs.
stub-prefix-lsa	(Optional) Configures the router to set the maximum metric for stub links in prefix LSAs.
summary-lsa	(Optional) Configures the router to override the summary LSA metric with the maximum metric value.

Command Default

Router link-state advertisements (LSAs) are originated with normal link metrics.

Command Modes

Router address family topology configuration (config-router-af-topology)
Router configuration (config-router)
OSPFv3 router configuration mode (config-router)

Command History

Release	Modification
12.0(15)S	This command was introduced.
12.0(16)ST	This command was integrated into Cisco IOS Release 12.0(16)ST.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.4(10)	The **include-stub**, **summary-lsa**, and **external-lsa** keywords and the *max-metric-value* argument were made available under router configuration mode.
12.4(11)T	The **include-stub**, **summary-lsa**, and **external-lsa** keywords and the *max-metric-value* argument were made available under router configuration mode.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(31)SB2	The **include-stub**, **summary-lsa**, and **external-lsa** keywords and the *max-metric-value* argument were made available under router configuration mode.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was made available in router address family topology configuration mode. The **include-stub**, **summary-lsa**, and **external-lsa** keywords and the *max-metric-value* argument were made available under router configuration mode.
15.1(3)S	This command was modified. Support for IPv6 and OSPF version 3 (OSPFv3) was added.
Cisco IOS XE Release 3.4S	This command was modified. Support for IPv6 and OSPF version 3 (OSPFv3) was added.

Usage Guidelines

Enabling the **max-metric router-lsa** command will cause a router to originate LSAs with a maximum metric (LSInfinity: 0xFFFF) through all nonstub links, which allows BGP routing tables to converge without attracting transit traffic (if there are not alternate lower cost paths around the router). The router will advertise accurate (normal) metrics after the configured or default timers expire or after BGP sends a notification that routing tables have converged.

Note Directly connected links in a stub network are not affected by the configuration of a maximum or infinite metric because the cost of a stub link is always set to the output interface cost.

The **max-metric router-lsa** command is useful in the following situations:

- Reloading a router. After a router is reloaded, Interior Gateway Protocols (IGPs) converge very quickly, and other routers may try to forward traffic through the newly reloaded router. If the router is still building BGP routing tables, packets destined for other networks that the router has not learned through BGP may be dropped. In the case of an Internet backbone router, a large number of packets may be dropped.
- Introducing a router into a network without routing traffic through it. You may want to connect a router to an OSPF network but not want real traffic flowing through the router if there are better alternate paths. If there are no alternate paths, this router would still accept transit traffic as before.
- Gracefully removing a router from a network. This feature allows you to gracefully remove a router from the network by advertising a maximum metric through all links, which allows other routers to select alternate paths for transit traffic to follow before the router is shut down.

Note You should not save the running configuration of a router when it is configured for a graceful shutdown because the router will continue to advertise a maximum metric after it is reloaded.

Note In older OSPF implementations (RFC 1247 and earlier implementations), the router link costs in received LSAs with a metric of LSInfinity are not used during SPF calculations, which means that no transit traffic will be sent to the routers that originate these LSAs.

Examples

The following example configures a router that is running OSPF to advertise a maximum metric for 100 seconds:

```
Router(config)# router ospfv3 100
Router(config-router)# max-metric router-lsa on-startup 100
```

The following example configures a router to advertise a maximum metric until BGP routing tables converge or until the default timer expires (600 seconds):

```
Router(config)# router ospfv3 100
Router(config-router)# max-metric router-lsa on-startup wait-for-bgp
```

The following example configures a router that is running OSPF to advertise a maximum metric, which causes neighbor routers to select alternate paths for transit traffic before the router shuts down:

```
Router(config)# router ospfv3 100
Router(config-router)# max-metric router-lsa
Router(config-router)# end
```

The following example configures stub links to be advertised with the maximum-metric in routers LSAs.

```
Router(config)# router ospfv3 1
Router(config-router)# router-id 10.1.1.1
Router(config-router)# max-metric router-lsa include-stub
Router(config-router)# end
```

Entering the **show ip ospf max-metric** or **show ospfv3 max-metric** command with the **include-stub** keyword displays output that confirms that stub links are advertised with the maximum metric. The example provides output for the **show ip ospf max-metric** command:

```
Router# show ip ospf max-metric

Routing Process "ospf 1" with ID 10.1.1.1
 Start time: 00:00:03.524, Time elapsed: 01:02:28.292
 Originating router-LSAs with maximum metric
    Condition: always, State: active
    Advertise stub links with maximum metric in router-LSAs
```

Related Commands

Command	Description
show ip ospf	Displays general information about OSPF routing processes.
show ip ospf database	Displays lists of information related to the OSPF database for a specific router.

maximum routes

To limit the maximum number of routes in a Virtual Private Network (VPN) routing and forwarding (VRF) instance to prevent a provider edge (PE) router from importing too many routes, use the **maximum routes** command in VRF configuration mode or in VRF address family configuration mode. To remove the limit on the maximum number of routes allowed, use the **no** form of this command.

maximum routes *limit* {**warning-only** | *warn-threshold* [**reinstall** *reinstall-threshold*]}

no maximum routes

Syntax Description

limit	The maximum number of routes allowed in a VRF. The valid range is from 1 to 4294967295 routes. All values within this range can be configured for IPv4. For IPv6, however, only values greater than the current number of IPv6 routes present in the Routing Information Base (RIB) for the specified VRF is allowed.
warn-threshold	The warning threshold value expressed as a percentage (from 1 to 100) of the *limit* value. When the number of routes reaches the specified percentage of the limit, a warning message is generated.
warning-only	Issues a system message logging (syslog) error message when the maximum number of routes allowed for a VRF exceeds the threshold. However, additional routes are still allowed.
reinstall *reinstall-threshold*	(Optional) Specifies reinstallation of a route previously rejected because the maximum route limit was exceeded. The *reinstall-threshold* is expressed as a percentage (from 1 to 100) of the *limit* value, but it does not take effect until the limit has been reached. When the number of routes reaches the specified percentage of the limit, a warning message is generated, but routes are still accepted. When the number of routes reaches the limit, the router rejects new routes and does not accept any more until the number of routes drops below the specified percentage of the *reinstall-threshold*.

Command Default

No limit is set on the maximum number of routes allowed.

Command Modes

VRF address family configuration (config-vrf-af)
VRF configuration (config-vrf)

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.2(13)T	Support for Simple Network Management Protocol (SNMP) notifications was added.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA. The **reinstall** *reinstall-threshold* keyword and argument were added.
12.2(33)SRB	Support for IPv6 was added.
12.2(33)SRC	Support for this command was added for IPv6 address families under the **vrf definition** command.
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.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

All values within the range for the *limit* argument can be configured for IPv4. For IPv6, however, only values greater than the current number of IPv6 routes present in the RIB for the specified VRF is allowed.

The **maximum routes** command can be configured in one of two ways:

- Generate a warning message when the *limit* value is exceeded
- Generate a warning message when the *warn-threshold* value is reached

To limit the number of routes allowed in the VRF, use the **maximum routes** *limit* command with the *warn-threshold* argument. The *warn-threshold* argument generates a warning and does not allow the addition of routes to the VRF when the maximum number set by the *limit* argument is reached. The software generates a warning message every time a route is added to a VRF when the VRF route count is above the warning threshold. The software also generates a route rejection notification when the maximum threshold is reached and every time a route is rejected after the limit is reached.

To set a number of routes at which you receive a notification, but which does not limit the number of routes that can be imported into the VRF, use the **maximum routes** *limit* command with the **warn-only** keyword.

To configure the router to generate SNMP notifications (traps or informs) for these values, use the **snmp-server enable traps mpls vpn** command in global configuration mode.

Examples

The following example shows how to set a limit threshold of VRF routes to 1000. When the number of routes for the VRF reaches 1000, the router issues a syslog error message, but continues to accept new VRF routes.

```
Router(config)# ip vrf vrf1
Router(config-vrf)# rd 100:1
Router(config-vrf)# route-target import 100:1
Router(config-vrf)# maximum routes 1000 warning-only
```

The following example shows how to set the maximum number of VRF routes allowed to 1000 and set the warning threshold at 80 percent of the maximum. When the number of routes for the VRF reaches 800, the router issues a warning message. When the number of routes for the VRF reaches 1000, the router issues a syslog error message and rejects any new routes.

```
Router(config)# ip vrf vrf2
Router(config-vrf)# rd 200:1
Router(config-vrf)# route-target import 200:1
Router(config-vrf)# maximum routes 1000 80
```

The following example shows how to use the **reinstall** keyword to control the maximum number of VRF routes allowed. In this example, the router issues a warning when the number of routes exceeds 800 (80% of 1000 routes), but it still accept routes. When the number of new routes reaches 1000 (the limit), the router rejects them and does not accept more until the number of routes drops below 900 (90% of 1000) installed routes.

```
Router(config)# ip vrf vrf2
Router(config-vrf)# rd 200:1
Router(config-vrf)# route-target import 200:1
Router(config-vrf)# maximum routes 1000 80 reinstall 90
```

The following example for an IPv6 address family defined under the **vrf definition** command shows how to set the maximum number of VRF routes allowed to 500 and set the warning threshold at 50 percent of the maximum. When the number of routes for the VRF reaches 250, the router issues a warning message. When the number of routes for the VRF reaches 500, the router issues a syslog error message and rejects any new routes.

```
Router(config)# vrf definition vrf1
Router(config-vrf)# address-family ipv6
Router(config-vrf-af)# maximum routes 500 50
```

Related Commands

Command	Description
address-family (VRF)	Selects an address family type for a VRF table and enters VRF address family configuration mode.
import map	Configures an import route map for a specified VRF for more control over routes imported into the VRF.
ip vrf	Specifies a name for a VRF routing table and enters VRF configuration mode (for IPv4 only).
rd	Creates VRF routing and forwarding tables and specifies the default route distinguisher for a VPN.
route-target	Configures a VRF route target community for importing and exporting extended community attributes.
snmp-server enable traps mpls vpn	Enables the router to send MPLS VPN-specific SNMP notifications (traps and informs).
vrf definition	Configures a VRF routing table instance and enters VRF configuration mode.

maximum-paths (IPv6)

To control the maximum number of equal-cost routes that a process for IPv6 Border Gateway Protocol (BGP), a process for IPv6 Intermediate System-to-Intermediate System (IS-IS), a process for IPv6 Routing Information Protocol (RIP), a process for Open Shortest Path First (OSPF) for IPv6, or a process for Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 routing can support, use the **maximum-paths** command in address family configuration or router configuration mode. To restore the default value, use the **no** form of this command.

maximum-paths *number-paths*

no maximum-paths

Syntax Description

number-paths	Maximum number of equal-cost paths to a destination learned via IPv6 BGP, IS-IS, RIP, OSPF, or EIGRP installed in the IPv6 routing table, in the range from 1 to 64.

Command Default

The default for BGP is 1 path, the default for IS-IS and RIP is 4 paths, and the default for OSPF for IPv6 is 16 paths.

Command Modes

Address family configuration
Router configuration

Command History

Release	Modification
12.2(8)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 and support for IPv6 RIP was added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	Support for IPv6 OSPF was added.
12.4(6)T	Support for EIGRP for IPv6 was 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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

To configure the **maximum-paths** command for IPv6 BGP and IS-IS, enter address family configuration mode.

Examples

The following example shows a maximum of three paths to an external destination for the IPv6 BGP autonomous system 65000, and a maximum of two paths to an IPv6 internal BGP destination being configured:

```
Router(config)# router bgp 65000
Router(config-router)# address-family ipv6
Router(config-router-af)# maximum-paths 3
Router(config-router-af)# maximum-paths ibgp 2
```

The following example shows a maximum of two paths to a destination for the IPv6 IS-IS routing process named area01 being configured:

```
Router(config)# router isis area01
Router(config-router)# address-family ipv6
Router(config-router-af)# maximum-paths 2
```

The following example shows a maximum of one path to a destination for the IPv6 RIP routing process named one being configured:

```
Router(config)# ipv6 router rip one
Router(config-router-rip)# maximum-paths 1
```

The following example shows a maximum of four paths to a destination for an IPv6 OSPF routing process:

```
Router(config) ipv6 router ospf 1
Router(config-router)# maximum-paths 4
```

The following example shows a maximum of two paths to a destination for an EIGRP for IPv6 routing process:

```
Router(config) ipv6 router eigrp 1
Router(config-router)# maximum-paths 2
```

Related Commands

Command	Description
address-family ipv6	Enters address family configuration mode for configuring routing sessions such as BGP that use standard IPv6 address prefixes.
ipv6 router eigrp	Configures the EIGRP routing process in IPv6.
ipv6 router ospf	Enables OSPF for IPv6 router configuration mode.
ipv6 router rip	Configures an IPv6 RIP routing process.
router bgp	Configures the BGP routing process.
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process.

maximum-paths (OSPFv3)

To control the maximum number of equal-cost routes that a process for Open Shortest Path First version 3 (OSPFv3) routing can support, use the **maximum-paths** command in IPv6 or IPv4 address family configuration mode. To restore the default value, use the **no** form of this command.

maximum-paths *number-paths*

no maximum-paths

Syntax Description

number-paths	Maximum number of equal-cost paths to a destination learned through OSPFv3. The range is from 1 through 64.

Command Default

16 equal-cost paths

Command Modes

IPv6 address family configuration (config-router-af)
IPv4 address family configuration (config-router-af)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

.

Examples

The following example shows how to configure a maximum of four paths to a destination for an OSPFv3 routing process:

```
Router(config-router)# address-family ipv6 unicast
Router(config-router-af)# maximum-paths 4
```

maximum-paths ibgp

To control the maximum number of parallel internal Border Gateway Protocol (iBGP) routes that can be installed in a routing table, use the **maximum-paths ibgp** command in router or address family configuration mode. To restore the default value, use the **no** form of this command.

Router Configuration Mode

maximum-paths ibgp *number-of-paths*

no maximum-paths ibgp *number-of-paths*

Under VRF in Address Family Configuration Mode

maximum-paths ibgp {*number-of-paths* [**import** *number-of-import-paths*] | **unequal-cost** *number-of-import-paths*}

no maximum-paths ibgp {*number-of-paths* [**import** *number-of-import-paths*] | **unequal-cost** *number-of-import-paths*}

Syntax Description

number-of-paths	Number of routes to install to the routing table. See the "Usage Guidelines" section for the number of paths that can be configured with this argument.
import *number-of-import-paths*	(Optional) Specifies the number of redundant paths that can be configured as backup multipaths for a virtual routing and forwarding (VRF) instance. This keyword can be configured only under a VRF in address family configuration mode. **Note** We recommend that this keyword is enabled only where needed and that the number of import paths be kept to the minimum (typically, not more than two paths). For more information, see the related note in the "Usage Guidelines" section of this command page.
unequal-cost *number-of-import-paths*	Specifies the number of unequal-cost routes to install in the routing table. See the "Usage Guidelines" section for the number of paths that can be configured. This keyword can be configured only under a VRF instance in address family configuration mode.

Command Default

BGP, by default, will install only one best path in the routing table.

Command Modes

Address family configuration (config-router-af)
Router configuration (config-router)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(25)S	The **import** keyword was added.

Release	Modification
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX.
12.3	The **import** keyword was added.
12.3(2)T	The maximum number of parallel routes was increased from 6 to 16.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S for use in IPv6.
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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.0(1)M	This command was modified. The **import** keyword was replaced by the **import path selection** and **import path limit** commands.
12.2(33)SRE	This command was modified. The **import** keyword was replaced by the **import path selection** and **import path limit** commands.
Cisco IOS XE 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

The **maximum-paths ibgp** command is used to configure equal-cost or unequal-cost multipath load sharing for iBGP peering sessions. In order for a route to be installed as a multipath in the BGP routing table, the route cannot have a next hop that is the same as another route that is already installed. The BGP routing process will still advertise a best path to iBGP peers when iBGP multipath load sharing is configured. For equal-cost routes, the path from the neighbor with the lowest router ID is advertised as the best path.

To configure BGP equal-cost multipath load sharing, all path attributes must be the same. The path attributes include weight, local preference, autonomous system path (entire attribute and not just the length), origin code, Multi Exit Discriminator (MED), and Interior Gateway Protocol (IGP) distance.

The number of paths that can be configured is determined by the version of Cisco IOS software as shown in the following list:

- Cisco IOS Release 12.0S-based software: 8 paths
- Cisco IOS Release 12.3T, 12.4, 12.4T, and 15.0-based software: 16 paths
- Cisco IOS Release 12.2S-based software: 32 paths

Note In IPv6, the **maximum-paths ibgp** command does not work for prefixes learned from iBGP neighbors that have been configured to distribute a Multiprotocol Label Switching (MPLS) label with its IPv6 prefix advertisements. If multiple routes exist for such prefixes, all of them are inserted into the Routing Information Base (RIB) when the **maximum-paths ibgp** command is configured, but only one is used and no load balancing occurs between equal-cost paths. The **maximum-paths ibgp** command works with 6PE only in Cisco IOS Release 12.2(25)S and subsequent 12.2S releases.

Configuring VRF Import Paths

A VRF will import only one path (the best path) per prefix from the source VRF table, unless the prefix is exported with a different route target. If the best path goes down, the destination will not be reachable until the next import event occurs, and then a new best path will be imported into the VRF table. The import event runs every 15 seconds by default.

The **import** keyword allows the network operator to configure the VRF table to accept multiple redundant paths in addition to the best path. An import path is a redundant path, and it can have a next hop that matches an installed multipath. This keyword should be used when multiple paths with identical next hops are available to ensure optimal convergence times. A typical application of this keyword is to configure redundant paths in a network that has multiple route reflectors for redundancy.

The maximum number of import paths that can be configured in Cisco IOS Release 12.2SY-based software is 16.

Note Configuring redundant paths with the **import** keyword can increase CPU and memory utilization significantly, especially in a network where there are many prefixes to learn and a large number of configured VRFs. It is recommended that this keyword be configured only as necessary and that the minimum number of redundant paths be configured (typically, not more than two).

In Cisco IOS Releases 15.0(1)M and 12.2(33)SRE, and in later releases, the **import** keyword was replaced by the **import path selection** and **import path limit** commands. If the **import** keyword is configured, the configuration is converted to the new commands, as show in the following example:

```
Router(config-router-af)# maximum-paths ibgp import 3
%NOTE: Import option has been deprecated.
%      Converting to 'import path selection all; import path limit 3'.
```

Examples

The following example configuration installs three parallel iBGP paths in a non-MPLS topology:

```
Router(config)# router bgp 100
Router(config-router)# maximum-paths ibgp 3
```

The following example configuration installs three parallel iBGP paths in an MPLS Virtual Private Network (VPN) topology:

```
Router(config)# router bgp 100
Router(config-router)# address-family ipv4 unicast vrf vrf-A
Router(config-route-af)# maximum-paths ibgp 3
```

The following example configuration installs two parallel routes in the VRF table:

```
Router(config)# router bgp 100
Router(config-router)# address-family ipv4 vrf vrf-B
Router(config-router-af)# maximum-paths ibgp 2 import 2
Router(config-router-af)# end
```

The following example configuration installs two parallel routes in the VRF table:

```
Router(config)# router bgp 100
Router(config-router)# address-family ipv4 vrf vrf-C
Router(config-router-af)# maximum-paths ibgp import 2
Router(config-router-af)# end
```

Related Commands

Command	Description
import path limit	Specifies the maximum number of BGP paths, per VRF importing net, that can be imported from an exporting net.
import path selection	Specifies the BGP import path selection policy for a specific VRF instance.
maximum-paths	Controls the maximum number of parallel routes an IP routing protocol can support.
maximum-paths ibgp	Configures the number of equal-cost or unequal-cost routes that BGP will install in the routing table.
show ip bgp	Displays entries in the BGP routing table.
show ip bgp vpnv4	Displays VPNv4 address information from the BGP table entries in the BGP routing table.

maximum sessions (DSP farm profile)

To specify the maximum number of sessions that are supported by the profile, use the **maximum sessions** command in DSP farm profile configuration mode. To reset to the default, use the **no** form of this command.

Command Syntax When Conferencing or Transcoding Is Configured

maximum sessions *number*

no maximum sessions

Command Syntax When MTP Is Configured

maximum sessions {**hardware** | **software**} *number*

no maximum sessions

Syntax Description

number	Number of session supported by the profile. Range is 0 to *x*. Default is 0. The *x* value is determined at run time depending on the number of resources available with the resource provider.
hardware	Number of sessions that media termination points (MTP) hardware resources will support.
software	Number of sessions that MTP software resources will support.

Command Default

The maximum number of supported sessions is 0.

Command Modes

DSP farm profile configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4(22)T	Support for IPv6 was added.

Usage Guidelines

When using the MTP service type, you must specify the number of sessions separately for software MTP and hardware MTP. The hardware MTP needs digital signal processor (DSP) resources. Use hardware MTP when the codecs are the same and the packetization period is different.

Active profiles must be shut down before any parameters can be changed.

Note The syntax of the command will vary based on the type of profile that you are configuring. The keywords work only when MTP is configured.

Examples

The following example shows that four sessions are supported by the DSP farm profile:

```
Router(config-dspfarm-profile)# maximum sessions
```

Related Commands

Command	Description
associate application	Associates the SCCP protocol to the DSP farm profile.
codec (dspfarm-profile)	Specifies the codecs supported by a DSP farm profile.
description (dspfarm-profile)	Includes a specific description about the DSP farm profile.
dspfarm profile	Enters DSP farm profile configuration mode and defines a profile for DSP farm services.
shutdown (dspfarm-profile)	Allocates DSP farm resources and associates with the application.
voice-card	Enters voice-card configuration mode.

metric weights (EIGRP)

To tune Enhanced Interior Gateway Routing Protocol (EIGRP) metric calculations, use the **metric weights** command in router configuration mode or address family configuration mode. To reset the values to their defaults, use the **no** form of this command.

metric weights *tos k1 k2 k3 k4 k5*

no **metric weights**

Syntax Description

tos	Type of service. This value must always be zero.
k1 k2 k3 k4 k5	Constants that convert an EIGRP metric vector into a scalar quantity. Valid values are 0 to 255. Default values are: • *tos:* 0 • *k1:* 1 • *k2:* 0 • *k3:* 1 • *k4:* 0 • *k5:* 0

Command Default

EIGRP metric K values are set to their default values.

Command Modes

Router configuration (config-router)
Address family configuration (config-router-af)

Command History

Release	Modification
10.0	This command was introduced.
12.4(6)T	Support for IPv6 was 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.
12.2SX	This command is supported in the Cisco 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 address-family configuration mode was added.
12.2(33)SRE	This command was modified. The address-family configuration mode was added.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was modified. The address-family configuration mode was added.

Usage Guidelines

Use this command to alter the default behavior of EIGRP routing and metric computation and allow the tuning of the EIGRP metric calculation for a particular type of service (ToS).

If k5 equals 0, the composite EIGRP metric is computed according to the following formula:

metric = [k1 * bandwidth + (k2 * bandwidth)/(256 - load) + k3 * delay]

If k5 does not equal zero, an additional operation is performed:

metric = metric * [k5/(reliability + k4)]

Bandwidth is inverse minimum bandwidth of the path in bps scaled by a factor of $2.56 * 10^{12}$. The range is from a 1200-bps line to 10 terabits per second.

Delay is in units of 10 microseconds. The range of delay is from 10 microseconds to 168 seconds. A delay of all ones indicates that the network is unreachable.

The delay parameter is stored in a 32-bit field, in increments of 39.1 nanoseconds. The range of delay is from 1 (39.1 nanoseconds) to hexadecimal FFFFFFFF (decimal 4,294,967,040 nanoseconds). A delay of all ones (that is, a delay of hexadecimal FFFFFFFF) indicates that the network is unreachable.

Table 36 lists the default values used for several common media.

Table 36 Bandwidth Values by Media Type

Media Type	Delay	Bandwidth
Satellite	51,200,000 (2 seconds)	5120 (500 megabits)
Ethernet	25600 (1 millisecond [ms])	256,000 (10 megabits)
1.544 Mbps	51,200,000 (20 ms)	1,657,856 bits
64 kbps	51,200,000 (20 ms)	40,000,000 bits
56 kbps	51,200,000 (20 ms)	45,714,176 bits
10 kbps	51,20,000 (20 ms)	256,000,000 bits
1 kbps	51,200,000 (20 ms)	2,560,000,000 bits

Reliability is given as a fraction of 255. That is, 255 is 100 percent reliability or a perfectly stable link.

Load is given as a fraction of 255. A load of 255 indicates a completely saturated link.

Examples

The following example sets the metric weights to slightly different values than the defaults:

```
Router(config)# router eigrp 109
Router(config-router)# network 192.168.0.0
Router(config-router)# metric weights 0 2 0 2 0 0
```

The following example configures an address-family metric weight to tos: 0; K1: 2; K2: 0; K3: 2; K4: 0; K5: 0.

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4533
Router(config-router-af)# metric weights 0 2 0 2 0 0
```

Related Commands

Command	Description
address-family (EIGRP)	Enters address-family configuration mode to configure an EIGRP routing instance.
bandwidth (interface)	Sets a bandwidth value for an interface.
delay (interface)	Sets a delay value for an interface.
ipv6 router eigrp	Configures the EIGRP for IPv6 routing process.
metric holddown	Keeps new EIGRP routing information from being used for a certain period of time.
metric maximum-hops	Causes the IP routing software advertise as unreachable routes with a hop count higher than is specified by the command (EIGRP only).
router eigrp	Configures the EIGRP address-family process.

mls cef maximum-routes

To limit the maximum number of the routes that can be programmed in the hardware allowed per protocol, use the **mls cef maximum-routes** command in global configuration mode. To return to the default settings, use the **no** form of this command.

mls cef maximum-routes {**ip** | **ip-multicast** | **ipv6** | **mpls**} *maximum-routes*

no mls cef maximum-routes {**ip** | **ip-multicast** | **ipv6** | **mpls**}

Syntax Description

ip	Specifies the maximum number of IP routes.
maximum-routes	Maximum number of the routes that can be programmed in the hardware allowed per protocol.
ip-multicast	Specifies the maximum number of multicast routes.
ipv6	Specifies the maximum number of IPv6 routes.
mpls	Specifies the maximum number of Multiprotocol Label Switching (MPLS) labels.

Command Default

The defaults are as follows:

- For XL-mode systems:
  - IPv4 unicast and MPLS—512,000 routes
  - IPv6 unicast and IPv4 multicast—256,000 routes
- For non-XL mode systems:
  - IPv4 unicast and MPLS—192,000 routes
  - IPv6 unicast and IPv4 multicast—32,000 routes

Note See the "Usage Guidelines" section for information on XL and non-XL mode systems.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(17b)SXA	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.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Note If you copy a configuration file that contains the multilayer switching (MLS) Cisco Express Forwarding maximum routes into the startup-config file and reload the Cisco 7600 series router, the Cisco 7600 series router reloads after it reboots.

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

The **mls cef maximum-routes** command limits the maximum number of the routes that can be programmed in the hardware. If routes are detected that exceed the limit for that protocol, an exception condition is generated.

The determination of XL and non-XL mode is based on the type of Policy Feature Card (PFC) or Distributed Forwarding Card (DFC) modules that are installed in your system. For additional information on systems running Cisco IOS software release 12.2SXF and earlier releases see:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/release/notes/OL_4164.html#Policy_Feature_Card_Guidelines_and_Restrictions

For additional information on systems running Cisco IOS software release 12.2SXH and later releases see:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/release/notes/ol_14271.html#Policy_Feature_Card_Guidelines_and_Restrictions

The valid values for the *maximum-routes* argument depend on the system mode—XL mode or non-XL mode. The valid values are as follows:

- XL mode
  - IP and MPLS—Up to 1,007,000 routes
  - IP multicast and IPv6—Up to 503,000 routes
- Non-XL mode
  - IP and MPLS—Up to 239,000 routes
  - IP multicast and IPv6—Up to 119,000 routes

Note The maximum values that you are permitted to configure is not fixed but varies depending on the values that are allocated for other protocols.

An example of how to enter the maximum routes argument is as follows:

```
mls cef maximum-routes ip 4
```

where 4 is 4096 IP routes (1024 x4 = 4096).

The new configurations are applied after a system reload only and do not take effect if a switchover occurs.

In RPR mode, if you change and save the maximum-routes configuration, the redundant supervisor engine reloads when it becomes active from either a switchover or a system reload. The reload occurs 5 minutes after the supervisor engine becomes active.

Use the **show mls cef maximum-routes** command to display the current maximum routes system configuration.

Examples

This example shows how to set the maximum number of routes that are allowed per protocol:

```
Router(config)# mls cef maximum-routes ip 100
```

This example shows how to return to the default setting for a specific protocol:

```
Router(config)# no mls cef maximum-routes ip
```

Related Commands

Command	Description
show mls cef maximum-routes	Displays the current maximum-route system configuration.

mls erm priority

To assign the priorities to define an order in which protocols attempt to recover from the exception status, use the **mls erm priority** command in global configuration mode. To return to the default settings, use the **no** form of this command.

Note The **mls erm priority** command is not available in Cisco IOS Release 12.2(33)SXJ and later Cisco IOS 12.2SX releases.

mls erm priority ipv4 *value* **ipv6** *value* **mpls** *value*

no mls erm priority ipv4 *value* **ipv6** *value* **mpls** *value*

Syntax Description

ipv4	Prioritizes the IPv4 protocol. The default priority is 1.
value	Priority value; valid values are from 1 to 3.
ipv6	Prioritizes the IPv6 protocol. The default priority is 2.
mpls	Prioritizes the Multiprotocol Label Switching (MPLS) protocol. The default priority is 3.

Command Default

The default priority settings are used.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)SX	This command was introduced on the Supervisor Engine 720.
12.2(17a)SX	This command was changed to support the **ipv6** keyword.
12.2(17b)SXA	This command was changed to support the **mpls** keyword.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXJ	This command was removed. It is not available in Cisco IOS Release 12.2(33)SXJ and later Cisco IOS 12.2SX releases.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

A lower *value* indicates a higher priority.

When a protocol sees a Forwarding Information Base (FIB) table exception, the protocol notifies the FIB Embedded Resource Manager (ERM). The FIB ERM periodically polls the FIB table exception status and decides which protocol gets priority over another protocol when multiple protocols are running under the exception. Only one protocol can attempt to recover from an exception at any time.

If there is sufficient FIB space, the protocol with the highest priority tries to recover first. Other protocols under the exception do not start to recover until the previous protocol completes the recovery process by reloading the appropriate FIB table.

Examples

This example shows how to set the ERM exception-recovery priority:

```
Router(config)# mls erm priority ipv4 2 ipv6 1 mpls 3
```

This example shows how to return to the default setting:

```
Router(config)# no mls erm priority ipv4 2 ipv6 1 mpls 3
```

Related Commands

Command	Description
show mls cef exception	Displays information about the Cisco Express Forwarding exception.

mls ipv6 acl compress address unicast

To enable the compression of compressible IPv6 addresses, use the **mls ipv6 acl compress address unicast** command in global configuration mode. To disable the compression of compressible IPv6 addresses, use the **no** form of this command.

mls ipv6 acl compress address unicast

no mls ipv6 acl compress address unicast

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled.

Command Modes

Global configuration

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 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Note Do not enable the compression mode if you have noncompressible address types in your network. Compressible address types and the address compression method are listed in Table 37.

Table 37 Compressible Address Types and Methods

Address Type	Compression Method
EUI-64 based on MAC address	This address is compressed by removing 16 bits from bit locations [39:24]. No information is lost when the hardware compresses these addresses.
Embedded IPv4 address	This address is compressed by removing the upper 16 bits. No information is lost when the hardware compresses these addresses.

Table 37 Compressible Address Types and Methods (continued)

Address Type	Compression Method
Link Local	These addresses are compressed by removing the zeros in bits [95:80] and are identified using the same packet type as the embedded IPv4 address. No information is lost when the hardware compresses these addresses.
Other	If the IPv6 address does not fall into any of the categories, it is classified as Other. If the IPv6 address is classified as Other, the following occurs: • If the compress mode is on, the IPv6 address is compressed similarly to the EUI-64 compression method (removal of bits [39:24]) to allow for the Layer 4 port information to be used as part of the key used to look up the quality of service (QoS) ternary content addressable memory (TCAM), but Layer 3 information is lost. • If the global compression mode is off, the entire 128 bits of the IPv6 address are used. The Layer 4 port information cannot be included in the key to look up the QoS TCAM because of the size constraints on the IPv6 lookup key.

Examples

This example shows how to turn on the compression of compressible IPv6 addresses:

```
Router(config)# mls ipv6 acl compress address unicast
```

This example shows how to turn off the compression of compressible IPv6 addresses:

```
Router(config)# no mls ipv6 acl compress address unicast
```

Related Commands

Command	Description
show fm ipv6 traffic-filter	Displays the IPv6 information.
show mls netflow ipv6	Displays configuration information about the NetFlow hardware.

mls ipv6 acl source

To deny all IPv6 packets from a source-specific address, use the **mls ipv6 acl source** command in global configuration mode. To accept all IPv6 packets from a source-specific address, use the **no** form of this command.

mls ipv6 acl source {**loopback** | **multicast**}

no mls ipv6 acl source {**loopback** | **multicast**}

Syntax Description

loopback	Denies all IPv6 packets with a source loopback address.
multicast	Denies all IPv6 packets with a source multicast address.

Command Default

This command is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(17b)SXA	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.

Examples

This example shows how to deny all IPv6 packets with a source loopback address:

```
Router(config)# mls ipv6 acl source loopback
```

This example shows how to deny all IPv6 packets with a source multicast address:

```
Router(config)# no mls ipv6 acl source multicast
```

Related Commands

Command	Description
show mls netflow ipv6	Displays configuration information about the NetFlow hardware.

mls ipv6 vrf

To enable IPv6 globally in a virtual routing and forwarding (VRF) instance, use the **mls ipv6 vrf** command in global configuration mode. To remove this functionality, use the **no** form of the command.

mls ipv6 vrf

no mls ipv6 vrf

Syntax Description

This command has no arguments or keywords.

Command Default

VRFs are supported only for IPv4 addresses.

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)SRB1	This command was introduced on the Cisco 7600 series routers.
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 and implemented on the Catalyst 6500 series switches.
Cisco IOS XE Release 3.1S	This command was introduced on Cisco ASR 1000 series routers.

Usage Guidelines

You must enable the **mls ipv6 vrf** command in global configuration mode in order to enable IPv6 in a VRF. If this command is not used, a VRF is supported only for the IPv4 address family.

Configuring the **mls ipv6 vrf** command makes the router reserve the lower 255 hardware IDs for IPv6 regardless of whether IPv6 is enabled. Other applications that make use of these hardware IDs then cannot use that space.

To remove the **mls ipv6 vrf** command from the running configuration, the user needs to remove all IPv6 VRFs from the router and reload the system.

Examples

The following example shows how to enable IPv6 in a VRF globally:

```
Router(config)# mls ipv6 vrf
```

Related Commands

Command	Description
vrf definition	Configure a VRF routing table instance and enters VRF configuration mode.
show running-config vrf	Displays the subset of the running configuration of a router that is linked to a specific VRF instance or to all VRFs configured on the router.

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 38 lists the IPv6 rate limiters and the class of traffic that each rate limiter serves.

Table 38 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.

monitor event-trace cef ipv6 (global)

To configure event tracing for Cisco Express Forwarding IPv6 events, use the **monitor event-trace cef ipv6** command in global configuration mode. To disable event tracing for Cisco Express Forwarding, use the **no** form of this command.

monitor event-trace cef ipv6 {**disable** | **distribution** | **dump-file** *dump-file-name* | **enable** | **match** {**global** | *ipv6-address/n*} | **size** *number* | **stacktrace** [*depth*] | **vrf** *vrf-name* [**distribution** | **match** {**global** | *ipv6-address/n*}]}

no monitor event-trace cef ipv6 {**disable** | **distribution** | **dump-file** *dump-file-name* | **enable** | **match** | **size** | **stacktrace** [*depth*] | **vrf**}

Syntax Description

disable	Turns off event tracing for Cisco Express Forwarding IPv6 events.
distribution	Logs events related to the distribution of Cisco Express Forwarding Forwarding Information Base (FIB) tables to the line cards.
dump-file *dump-file-name*	Specifies the file to which event trace messages are written from memory on the networking device. The maximum length of the filename (path and filename) is 100 characters, and the path can point to flash memory on the networking device or to a TFTP or FTP server.
enable	Turns on event tracing for Cisco Express Forwarding IPv6 events if it had been enabled with the **monitor event-trace cef ipv6** command.
match	Turns on event tracing for Cisco Express Forwarding IPv6 that matches global events or events that match a specific network address.
global	Specifies global events.
ipv6-address/n	Specifies an IPv6 address. This address must be in the form documented in RFC 2373: the address is specified in hexadecimals using 16-bit values between colons. The slash followed by a number (*/n*) indicates the number of bits that do not change. Range: 0 to 128.
size *number*	Sets the number of messages that can be written to memory for a single instance of a trace. Range: 1 to 65536. **Note** Some Cisco IOS software subsystem components set the size by default. To display the size parameter, use the **show monitor event-trace cef parameters** command. When the number of event trace messages in memory exceeds the configured size, new messages will begin to overwrite the older messages in the file.
stacktrace	Enables the stack trace at tracepoints.
depth	(Optional) Specifies the depth of the stack trace stored. Range: 1 to 16.
vrf *vrf-name*	Turns on event tracing for a Cisco Express Forwarding IPv6 Virtual Private Network (VPN) routing and forwarding (VRF) table. The *vrf-name* argument specifies the name of the VRF.

Command Default

Event tracing for Cisco Express Forwarding IPv6 events is enabled by default.

Command Modes Global configuration (config)

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.
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 and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines Use the **monitor event-trace cef ipv6** command to enable or disable event tracing for Cisco Express Forwarding IPv6 events.

The Cisco IOS software allows Cisco Express Forwarding to define whether support for event tracing is enabled or disabled by default. The command interface for event tracing allows you to change the default value in one of two ways: using the **monitor event-trace cef ipv6** command in privileged EXEC mode or using the **monitor event-trace cef ipv6** command in global configuration mode.

Note The amount of data collected from the trace depends on the trace message size configured using the **monitor event-trace cef ipv6** command for each instance of a trace.

To determine whether event tracing is enabled by default for Cisco Express Forwarding IPv6 events, use the **show monitor event-trace cef ipv6** command to display trace messages.

To specify the trace call stack at tracepoints, you must first clear the trace buffer.

Examples The following example shows how to enable event tracing for Cisco Express Forwarding IPv6 events and configure the buffer size to 10000 messages.

```
Router(config)# monitor event-trace cef ipv6 enable

Router(config)# monitor event-trace cef ipv6 size 10000
```

Related Commands

Command	Description
monitor event-trace cef (EXEC)	Monitors and controls the event trace function for Cisco Express Forwarding.
monitor event-trace cef (global)	Configures event tracing for Cisco Express Forwarding.
monitor event-trace cef ipv4 (global)	Configures event tracing for Cisco Express Forwarding IPv4 events.
show monitor event-trace cef	Displays event trace messages for Cisco Express Forwarding.
show monitor event-trace cef events	Displays event trace messages for Cisco Express Forwarding events.

Command	Description
show monitor event-trace cef interface	Displays event trace messages for Cisco Express Forwarding interface events.
show monitor event-trace cef ipv4	Displays event trace messages for Cisco Express Forwarding IPv4 events.
show monitor event-trace cef ipv6	Displays event trace messages for Cisco Express Forwarding IPv6 events.

monitor event-trace ipv6 spd

To monitor Selective Packet Discard (SPD) state transition events, use the **monitor event-trace ipv6 spd** command in privileged EXEC mode. To disable this function, use the **no** form of this command.

monitor event-trace ipv6 spd

no monitor event-trace ipv6 spd

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

Use the **monitor event-trace ipv6 spd** command to check SPD state transition events.

mpls ipv6 source-interface

Note Effective with Cisco IOS Release 12.2(25)S, the **mpls ipv6 source-interface** command is not available in Cisco IOS 12.2S releases.
Effective with Cisco IOS Release 12.4(15)T, the **mpls ipv6 source-interface** command is not available in Cisco IOS 12.4T releases.

To specify an IPv6 address of an interface to be used as the source address for locally generated IPv6 packets to be sent over a Multiprotocol Label Switching (MPLS) network, use the **mpls ipv6 source-interface** command in global configuration mode. To disable this feature, use the **no** form of this command.

mpls ipv6 source-interface *type number*

no mpls ipv6 source-interface

Syntax Description

type number	The interface type and number whose IPv6 address is to be used as the source for locally generated IPv6 packets to be sent over an MPLS backbone. **Note** A space between the *type* and *number* arguments is not required.

Command Default

This command is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(20)S	This command was integrated into Cisco IOS Release 12.2(20)S.
12.2(25)S	This command was removed from Cisco IOS Release 12.2(25)S.
12.4(15)T	This command was removed from Cisco IOS Release 12.4(15)T.

Usage Guidelines

Use the **mpls ipv6 source-interface** command with the **neighbor send-label** address family configuration command to allow IPv6 traffic to run over an IPv4 MPLS network without any software or hardware configuration changes in the backbone. Edge routers, configured to run both IPv4 and IPv6, forward IPv6 traffic using MPLS and multiprotocol internal BGP (MP-iBGP).

The **mpls ipv6 source-interface** command was removed from Cisco IOS software as per RFC 3484, which defines how the source address of a locally generated packet must be chosen. This command will be removed from the other Cisco IOS release trains in which it currently appears.

Examples

The following example shows loopback interface 0 being configured as a source address for locally generated IPv6 packets:

```
interface Loopback0
 ip address 192.168.99.5 255.255.255.255
 ipv6 address 2001:0DB8::1/32
!
mpls ipv6 source-interface loopback0
```

Related Commands

Command	Description
neighbor send-label	Advertises the capability of the router to send MPLS labels with BGP routes.

mpls ldp router-id

To specify a preferred interface for the Label Distribution Protocol (LDP) router ID, use the **mpls ldp router-id** command in global configuration mode. To disable the interface from being used as the LDP router ID, use the **no** form of this command.

mpls ldp router-id [**vrf** *vrf-name*] *interface* [**force**]

no mpls ldp router-id [**vrf** *vrf-name*] [*interface* [**force**]]

Cisco CMTS Routers

mpls ldp router-id gigabitethernet *slot*/*subslot*/*port* [**force**]

no mpls ldp router-id gigabitethernet *slot*/*subslot*/*port* [**force**]

Syntax Description

vrf *vrf-name*	(Optional) Selects the interface as the LDP router ID for the named Virtual Private Network (VPN) routing and forwarding (VRF) table. The selected interface must be associated with the named VRF.
interface	The specified interface to be used as the LDP router ID, provided that the interface is operational.
gigabitethernet *slot*/*subslot*/*port*	Specifies the location of the Gigabit Ethernet interface.
force	(Optional) Alters the behavior of the **mpls ldp router-id** command, as described in the "Usage Guidelines" section.

Command Default

If the **mpls ldp router-id** command is not executed, the router determines the LDP router ID as follows:

1. The router examines the IP addresses of all operational interfaces.
2. If these IP addresses include loopback interface addresses, the router selects the largest loopback address as the LDP router ID.
3. Otherwise, the router selects the largest IP address pertaining to an operational interface as the LDP router ID.

Command Modes

Global configuration

Command History

Release	Modification
12.0(10)ST	This command was introduced.
12.0(14)ST	The **force** keyword was added.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.4(5)	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.

Release	Modification
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(33)SCC	This command was integrated into Cisco IOS Release 12.2(33)SCC.

Usage Guidelines

The **mpls ldp router-id** command allows you to use the IP address of an interface as the LDP router ID.

The following steps describe the normal process for determining the LDP router ID:

1. The router considers all the IP addresses of all operational interfaces.
2. If these addresses include loopback interface addresses, the router selects the largest loopback address. Configuring a loopback address helps ensure a stable LDP ID for the router, because the state of loopback addresses does not change. However, configuring a loopback interface and IP address on each router is not required.

   The loopback IP address does not become the router ID of the local LDP ID under the following circumstances:

   – If the loopback interface has been explicitly shut down.

   – If the **mpls ldp router-id** command specifies that a different interface should be used as the LDP router ID.

   If you use a loopback interface, make sure that the IP address for the loopback interface is configured with a /32 network mask. In addition, make sure that the routing protocol in use is configured to advertise the corresponding /32 network.
3. Otherwise, the router selects the largest interface address.

The router might select a router ID that is not usable in certain situations. For example, the router might select an IP address that the routing protocol cannot advertise to a neighboring router.

The router implements the router ID the next time it is necessary to select an LDP router ID. The effect of the command is delayed until the next time it is necessary to select an LDP router ID, which is typically the next time the interface is shut down or the address is deconfigured.

If you use the **force** keyword with the **mpls ldp router-id** command, the router ID takes effect more quickly. However, implementing the router ID depends on the current state of the specified interface:

- If the interface is up (operational) and its IP address is not currently the LDP router ID, the LDP router ID is forcibly changed to the IP address of the interface. This forced change in the LDP router ID tears down any existing LDP sessions, releases label bindings learned via the LDP sessions, and interrupts MPLS forwarding activity associated with the bindings.
- If the interface is down, the LDP router ID is forcibly changed to the IP address of the interface when the interface transitions to up. This forced change in the LDP router ID tears down any existing LDP sessions, releases label bindings learned via the LDP sessions, and interrupts MPLS forwarding activity associated with the bindings.

The following behaviors apply to the default VRF as well as to VRFs that you explicitly configure with the **vrf** *vrf-name* keyword/argument pair:

- The interface you select as the router ID of the VRF must be associated with the VRF.
- If the interface is no longer associated with the VRF, the **mpls ldp router-id** command that uses the interface is removed.
- If the selected interface is deleted, the **mpls ldp router-id** command that uses the interface is removed.

- If you delete a VRF that you configured, the **mpls ldp router-id** command for the deleted VRF is removed. The default VRF cannot be deleted.

Examples

The following example shows that the POS2/0/0 interface has been specified as the preferred interface for the LDP router ID. The IP address of that interface is used as the LDP router ID.

```
Router(config)# mpls ldp router-id pos2/0/0
```

The following example shows that the Ethernet 1/0 interface, which is associated with the VRF vpn-1, is the preferred interface. The IP address of the interface is used as the LDP router ID.

```
Router(config)# mpls ldp router-id vrf vpn-1 eth1/0
```

Related Commands

Command	Description
show mpls ldp discovery	Displays the status of the LDP discovery process.

mpls traffic-eng auto-bw timers

To enable automatic bandwidth adjustment for a platform and to start output rate sampling for tunnels configured for automatic bandwidth adjustment, use the **mpls traffic-eng auto-bw timers** command in global configuration mode. To disable automatic bandwidth adjustment for the platform, use the **no** form of this command.

mpls traffic-eng auto-bw timers [**frequency** *seconds*]

no mpls traffic-eng auto-bw timers

Syntax Description

frequency *seconds*	(Optional) Interval, in seconds, for sampling the output rate of each tunnel configured for automatic bandwidth. The value must be from 1 through 604800. The recommended value is 300.

Command Default

When the optional **frequency** keyword is not specified, the sampling interval is 300 seconds (5 minutes).

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(11)S	This command was integrated into Cisco IOS Release 12.2(11)S.
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.
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.

Usage Guidelines

The **mpls traffic-eng auto-bw timers** command enables automatic bandwidth adjustment on a platform by causing traffic engineering to periodically sample the output rate for each tunnel configured for bandwidth adjustment.

The **no mpls traffic-eng auto-bw timers** command disables automatic bandwidth adjustment for a platform by terminating the output rate sampling and bandwidth adjustment for tunnels configured for adjustment. In addition, the **no** form of the command restores the configured bandwidth for each tunnel where "configured bandwidth" is determined as follows:

- If the tunnel bandwidth was explicitly configured via the **tunnel mpls traffic-eng bandwidth** command after the running configuration was written (if at all) to the startup configuration, the "configured bandwidth" is the bandwidth specified by that command.
- Otherwise, the "configured bandwidth" is the bandwidth specified for the tunnel in the startup configuration.

Examples

The following example shows how to designate that for each Multiprotocol Label Switching (MPLS) traffic engineering tunnel, the output rate is sampled once every 10 minutes (every 600 seconds):

```
Router(config)# mpls traffic-eng auto-bw timers frequency 600
```

Related Commands

Command	Description
tunnel mpls traffic-eng auto-bw	Enables automatic bandwidth adjustment for a tunnel, specifies the frequency with which tunnel bandwidth can be automatically adjusted, and designates the allowable range of bandwidth adjustments.
tunnel mpls traffic-eng bandwidth	Configures bandwidth required for an MPLS traffic engineering tunnel.

multi-topology

To enable multitopology Intermediate System-to-Intermediate System (IS-IS) for IPv6, use the **multi-topology** command in address family configuration mode. To disable multitopology IS-IS for IPv6, use the **no** form of this command.

multi-topology [**transition**]

no multi-topology

Syntax Description

transition	(Optional) Allows an IS-IS IPv6 user to continue to use single shortest path first (SPF) mode while upgrading to multitopology IS-IS for IPv6.

Command Default

Multitopology IS-IS is disabled by default.

Command Modes

Address family configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
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.
12.2(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 2.6	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

By default, the router runs IS-IS IPv6 in single SPF mode. The **multi-topology** command enables multitopology IS-IS for IPv6.

The optional **transition** keyword can be used to migrate from IS-IS IPv6 single SPF mode to multitopology IS-IS IPv6. When transition mode is enabled, the router advertises both multitopology type, length, and value (TLV) objects and single-SPF-mode IS-IS IPv6 TLVs, but the SPF is computed using the single-SPF-mode IS-IS IPv6 TLV. This action has the side effect of increasing the link-state packet (LSP) size.

Examples

The following example enables multitopology IS-IS for IPv6:

```
Router(config)# router isis
Router(config-router)# address-family ipv6
Router(config-router-af)# multi-topology
```

nai

To specify the network address identifier (NAI) for the IPv6 mobile node, use the **nai** command in home agent configuration mode or IPv6 mobile router host configuration mode. To remove a host configuration, use the **no** form of this command.

nai [**realm** | **user** | **macaddress**] {*user@realm* | *@realm*}

no nai

Syntax Description

realm	(Optional) A realm is to be used as the NAI.
user	(Optional) A user address is to be used as the NAI.
macaddress	(Optional) A MAC address is to be used as the NAI.
user@realm	Fully qualified specific user address and realm.
@realm	Any user address at a specific realm.

Command Default

No NAI is specified.

Command Modes

Home agent configuration (config-ha)
IPv6 mobile router host configuration (IPv6-mobile-router-host-config)

Command History

Release	Modification
12.4(11)T	This command was introduced.
12.2(33)SRB	Support for IPv6 was added.
12.4(20)T	IPv6 network mobility (NEMO) functionality was added.

Usage Guidelines

The **nai** command can be used to configure a specific user NAI or a generic realm for defining a group.

When the **address** command is configured with a specific IPv6 address, the **nai** command cannot be configured using the *@realm* argument. For example, the following **nai** command configuration would not be valid because the **address** command is configured with the specific address baba::1:

```
host group group1
  nai  @cisco.com
  address baba::1
```

Two different profiles cannot be configured with the **nai** command configured with the same *@realm* value. For example, the following two profiles are configured with the same NAI realm of @cisco.com, which is not valid:

```
host group group1
  nai  @cisco.com

host group group2
  nai  @cisco.com
```

However, if the one of the profiles uses a fully qualified NAI, which is configured using the **nai** command with the *user@realm* argument, its properties take precedence over the group profile for that user, and the second group's configuration using the **nai** command with the *@realm* argument is valid.

```
host group group1
  nai example@cisco.com
host group group2
  nai  @cisco.com
```

Examples

In the following example, the host group named group1 is configured using the NAI fully qualified realm of example@cisco.com:

```
host group group1
  nai example@cisco.com
```

Related Commands

Command	Description
host group	Creates a host configuration in IPv6 Mobile.
ipv6 mobile home-agent (global configuration)	Enters home agent configuration mode.

neighbor (EIGRP)

To define a neighboring router with which to exchange routing information on a router that is running Enhanced Interior Gateway Routing Protocol (EIGRP), use the **neighbor** command in router configuration mode or address-family configuration mode. To remove an entry, use the **no** form of this command.

neighbor {*ip-address* | *ipv6-address*} *interface-type interface-number* [**remote** *maximum-hops*]

no neighbor {*ip-address* | *ipv6-address*} *interface-type interface-number*

Syntax Description

ip-address	IP address of a peer router with which routing information will be exchanged.
ipv6-address	IPv6 address of a peer router with which routing information will be exchanged.
interface-type	Interface through which peering is established.
interface-number	Number of the interface or subinterface.
remote	(Optional) Specifies that the neighbor is remote. This keyword is available only for loopback interfaces.
maximum-hops	(Optional) Maximum hop count. Valid range is 3 to 100. This argument is available only when the **remote** keyword is configured.

Command Default

No neighboring routers are defined.

Command Modes

Router configuration (config-router)
Address-family configuration (config-router-af)

Command History

Release	Modification
10.0	This command was introduced.
12.4(6)T	The *ipv6-address* argument was 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.
12.2SX	This command is supported in the Cisco 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. Address-family configuration mode was added.
12.2(33)SRE	This command was modified. Address-family configuration mode was added.
Cisco IOS XE Release 2.5.	This command was modified. Address-family configuration mode was added.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

Multiple neighbor statements can be used to establish peering sessions with specific EIGRP neighbors. The interface through which EIGRP will exchange routing updates must be specified in the neighbor statement. The interfaces through which two EIGRP neighbors exchange routing updates must be configured with IP addresses from the same network.

Note Configuring the **passive-interface** command suppresses all incoming and outgoing routing updates and hello messages. EIGRP neighbor adjacencies cannot be established or maintained over an interface that is configured as passive.

Examples

The following example configures EIGRP peering sessions with the 192.168.1.1 and 192.168.2.2 neighbors:

```
Router(config)# router eigrp 1
Router(config-router)# network 192.168.0.0
Router(config-router)# neighbor 192.168.1.1 Ethernet 0/0
Router(config-router)# neighbor 192.168.2.2 Ethernet 1/1
```

The following named configuration example configures EIGRP to send address-family updates to specific neighbors:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# neighbor 192.168.1.1 ethernet0/0
Router(config-router-af)# neighbor 10.1.1.2 loopback0 remote 10
```

Related Commands

Command	Description
address-family (EIGRP)	Enters address-family configuration mode to configure an EIGRP routing instance.
ipv6 router eigrp	Configures the EIGRP for IPv6 routing process.
passive-interface	Disables sending EIGRP hello packets and disables routing updates on an interface.
router eigrp	Configures the EIGRP address-family process.

neighbor activate

To enable the exchange of information with a Border Gateway Protocol (BGP) neighbor, use the **neighbor activate** command in address family configuration mode or router configuration mode. To disable the exchange of an address with a BGP neighbor, use the **no** form of this command.

neighbor {*ip-address* | *peer-group-name* | *ipv6-address***%**} **activate**

no neighbor {*ip-address* | *peer-group-name* | *ipv6-address***%**} **activate**

Syntax Description

ip-address	IP address of the neighboring router.
peer-group-name	Name of the BGP peer group.
ipv6-address	IPv6 address of the BGP neighbor.
%	(Optional) IPv6 link-local address identifier. This keyword needs to be added whenever a link-local IPv6 address is used outside the context of its interface.

Command Default

The exchange of addresses with BGP neighbors is enabled for the IPv4 address family. Enabling address exchange for all other address families is disabled.

Note Address exchange for address family IPv4 is enabled by default for each BGP routing session configured with the **neighbor remote-as** command unless you configure the **no bgp default ipv4-activate** command before configuring the **neighbor remote-as** command, or you disable address exchange for address family IPv4 with a specific neighbor by using the **no** form of the **neighbor activate** command.

Command Modes

Address family configuration (config-router-af)
Router configuration (config-router)

Command History

Release	Modification
11.0	This command was introduced.
12.0(5)T	Support for address family configuration mode and the IPv4 address family was added.
12.2(2)T	The *ipv6-address* argument and support for the IPv6 address family were added.
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 Release 12.2(14)S.
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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	The **%** keyword was added

Release	Modification
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

Use this command to advertise address information in the form of an IP or IPv6 prefix. The address prefix information is known as Network Layer Reachability Information (NLRI) in BGP.

The **%** keyword is used whenever link-local IPv6 addresses are used outside the context of their interfaces. This keyword does not need to be used for non-link-local IPv6 addresses.

Examples

Address Exchange Example for Address Family vpn4

The following example shows how to enable address exchange for address family vpnv4 for all neighbors in the BGP peer group named PEPEER and for the neighbor 10.0.0.44:

```
Router(config)# address-family vpnv4
Router(config-router-af)# neighbor PEPEER activate
Router(config-router-af)# neighbor 10.0.0.44 activate
Router(config-router-af)# exit-address-family
```

Address Exchange Example for Address Family IPv4 Unicast

The following example shows how to enable address exchange for address family IPv4 unicast for all neighbors in the BGP peer group named group1 and for the BGP neighbor 172.16.1.1:

```
Router(config)# address-family ipv4 unicast
Router(config-router-af)# neighbor group1 activate
Router(config-router-af)# neighbor 172.16.1.1 activate
```

Address Exchange Example for Address Family IPv6

The following example shows how to enable address exchange for address family IPv6 for all neighbors in the BGP peer group named group2 and for the BGP neighbor 7000::2:

```
Router(config)# address-family ipv6
Router(config-router-af)# neighbor group2 activate
Router(config-router-af)# neighbor 7000::2 activate
```

Related Commands

Command	Description
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard IPv4 address prefixes.
address-family ipv6	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard IPv6 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard VPNv4 address prefixes.
address-family vpnv6	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard VPNv6 address prefixes.

exit-address-family	Exits from the address family submode.
neighbor remote-as	Adds an entry to the BGP or multiprotocol BGP neighbor table.

neighbor ebgp-multihop

To accept and attempt BGP connections to external peers residing on networks that are not directly connected, use the **neighbor ebgp-multihop** command in router configuration mode. To return to the default, use the **no** form of this command.

neighbor {*ip-address* | *ipv6-address* | *peer-group-name*} **ebgp-multihop** [*ttl*]

no neighbor {*ip-address* | *ipv6-address* | *peer-group-name*} **ebgp-multihop**

Syntax Description

ip-address	IP address of the BGP-speaking neighbor.
ipv6-address	IPv6 address of the BGP-speaking neighbor.
peer-group-name	Name of a BGP peer group.
ttl	(Optional) Time-to-live in the range from 1 to 255 hops.

Command Default

Only directly connected neighbors are allowed.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
10.0	This command was introduced.
11.0	The *peer-group-name* argument was added.
12.2(33)SRA	The *ipv6-address* argument and support for the IPv6 address family were 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.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

This feature should be used only under the guidance of Cisco technical support staff.

If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command.

To prevent the creation of loops through oscillating routes, the multihop will not be established if the only route to the multihop peer is the default route (0.0.0.0).

Examples

The following example allows connections to or from neighbor 10.108.1.1, which resides on a network that is not directly connected:

```
router bgp 109
 neighbor 10.108.1.1 ebgp-multihop
```

Related Commands

Command	Description
neighbor advertise-map non-exist-map	Allows a BGP speaker (the local router) to send the default route 0.0.0.0 to a neighbor for use as a default route.
neighbor peer-group (creating)	Creates a BGP peer group.
network (BGP and multiprotocol BGP)	Specifies the list of networks for the BGP routing process.

neighbor next-hop-unchanged

To enable an external BGP (eBGP) peer that is configured as multihop to propagate the next hop unchanged, use the **neighbor next-hop-unchanged** command in address family or router configuration mode. To disable that propagation of the next hop being unchanged, use the **no** form of this command.

neighbor {*ip-address* | *ipv6-address* | *peer-group-name*} **next-hop-unchanged** [**allpaths**]

no neighbor {*ip-address* | *ipv6-address* | *peer-group-name*} **next-hop-unchanged** [**allpaths**]

Syntax Description

ip-address	Propagate the iBGP path's next hop unchanged for this IPv4 neighbor.
ipv6-address	Propagate the iBGP path's next hop unchanged for this IPv6 neighbor.
peer-group-name	Propagate the iBGP path's next hop unchanged for this BGP peer group.
allpaths	(Optional) Propagate the next hop unchanged, for all paths (iBGP and eBGP) to this neighbor.

Command Default

This command is disabled by default.

Command Modes

Address family configuration (config-router-af)
Router configuration (config-router)

Command History

Release	Modification
12.0(16)ST	This command was introduced.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was modified. The **allpaths** keyword 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.
Cisco IOS XE 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

By default, for eBGP, the next hop to reach a connected network is the IP address of the neighbor that sent the update. Therefore, as an update goes from router to router, the next hop typically changes to be the address of the neighbor that sent the update (the router's own address).

However, there might be a scenario where you want the next hop to remain unchanged. The **neighbor next-hop-unchanged** command is used to propagate the next hop unchanged for multihop eBGP peering sessions. This command is configured on an eBGP neighbor, but the neighbor propagates routes learned from iBGP; that is, the neighbor propagates the next hop of iBGP routes toward eBGP.

Caution Using the **neighbor next-hop-unchanged** command or incorrectly altering the BGP next hop can cause inconsistent routing, routing loops, or a loss of connectivity. It should only be attempted by someone who has a good understanding of the design implications.

This command can be used to configure MPLS VPNs between service providers by not modifying the next hop attribute when advertising routes to an eBGP peer.

Examples

The following example configures a multihop eBGP peer at 10.0.0.100 in a remote autonomous system (AS). When the local router sends updates to that peer, it will send them without modifying the next hop attribute.

```
router bgp 65535
 address-family ipv4
 neighbor 10.0.0.100 remote-as 65600
 neighbor 10.0.0.100 activate
 neighbor 10.0.0.100 ebgp-multihop 255
 neighbor 10.0.0.100 next-hop-unchanged
 end
```

Related Commands

Command	Description
address-family ipv4	Enters address family configuration mode for configuring routing sessions, such as BGP, RIP, or static routing sessions, that use standard IPv4 address prefixes.
address-family vpnv4	Enters address family configuration mode for configuring routing sessions, such as BGP, RIP, or static routing sessions, that use standard VPNv4 address prefixes.
neighbor ebgp-multihop	Accepts and attempts BGP connections to external peers residing on networks that are not directly connected.
neighbor next-hop-self	Configures the router as the next hop for a BGP-speaking neighbor or peer group.

neighbor override-capability-neg

To enable the IPv6 address family for a Border Gateway Protocol (BGP) neighbor that does not support capability negotiation, use the **neighbor override-capability-neg** command in address family configuration mode. To disable the IPv6 address family for a BGP neighbor that does not support capability negotiation, use the **no** form of this command.

neighbor {*peer-group-name* | *ipv6-address*} **override-capability-neg**

no neighbor {*peer-group-name* | *ipv6-address*} **override-capability-neg**

Syntax Description

peer-group-name	Name of a BGP peer group.
ipv6-address	IPv6 address of the BGP neighbor. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

Command Default

Capability negotiation is enabled.

Command Modes

Address family configuration

Command History

Release	Modification
12.2(2)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 Release 12.2(14)S.
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.
12.2(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

Capability negotiation is used to establish a connection between BGP-speaking peers. If one of the BGP peers does not support capability negotiation, the connection is automatically terminated. The **neighbor override-capability-neg** command overrides the capability negotiation process and enables BGP-speaking peers to establish a connection.

The **neighbor override-capability-neg** command is supported only in address family configuration mode for the IPv6 address family.

Examples

The following example enables the IPv6 address family for BGP neighbor 7000::2:

```
Router(config)# address-family ipv6
Router(config-router-af)# neighbor 7000::2 override-capability-neg
```

The following example enables the IPv6 address family for all neighbors in the BGP peer group named group1:

```
Router(config)# address-family ipv6
Router(config-router-af)# neighbor group1 override-capability-neg
```

Related Commands

Command	Description
address-family ipv6	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard IPv6 address prefixes.

neighbor peer-group (assigning members)

To configure a BGP neighbor to be a member of a peer group, use the **neighbor peer-group** command in address family or router configuration mode. To remove the neighbor from the peer group, use the **no** form of this command.

neighbor {*ip-address* | *ipv6-address*} **peer-group** *peer-group-name*

no neighbor {*ip-address* | *ipv6-address*} **peer-group** *peer-group-name*

Syntax Description

ip-address	IP address of the BGP neighbor that belongs to the peer group specified by the *peer-group-name* argument.
ipv6-address	IPv6 address of the BGP neighbor that belongs to the peer group specified by the *peer-group-name* argument.
peer-group-name	Name of the BGP peer group to which this neighbor belongs.

Defaults

There are no BGP neighbors in a peer group.

Command Modes

Address family configuration (config-router-af)
Router configuration (config-router)

Command History

Release	Modification
11.0	This command was introduced.
12.0(7)T	Address family configuration mode was added.
12.2(2)T	Support for IPv6 was added.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
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.

Usage Guidelines

The neighbor at the IP address indicated inherits all the configured options of the peer group.

Note Using the **no** form of the **neighbor peer-group** command removes all of the BGP configuration for that neighbor, not just the peer group association.

Examples

The following router configuration mode example assigns three neighbors to the peer group named internal:

```
router bgp 100
 neighbor internal peer-group
 neighbor internal remote-as 100
 neighbor internal update-source loopback 0
 neighbor internal route-map set-med out
 neighbor internal filter-list 1 out
 neighbor internal filter-list 2 in
 neighbor 172.16.232.53 peer-group internal
 neighbor 172.16.232.54 peer-group internal
 neighbor 172.16.232.55 peer-group internal
 neighbor 172.16.232.55 filter-list 3 in
```

The following address family configuration mode example assigns three neighbors to the peer group named internal:

```
router bgp 100
address-family ipv4 unicast
 neighbor internal peer-group
 neighbor internal remote-as 100
 neighbor internal update-source loopback 0
 neighbor internal route-map set-med out
 neighbor internal filter-list 1 out
 neighbor internal filter-list 2 in
 neighbor 172.16.232.53 peer-group internal
 neighbor 172.16.232.54 peer-group internal
 neighbor 172.16.232.55 peer-group internal
 neighbor 172.16.232.55 filter-list 3 in
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
neighbor peer-group (creating)	Creates a BGP peer group.
neighbor shutdown	Disables a neighbor or peer group.

neighbor peer-group (creating)

To create a BGP or multiprotocol BGP peer group, use the **neighbor peer-group** command in address family or router configuration mode. To remove the peer group and all of its members, use the **no** form of this command.

neighbor *peer-group-name* **peer-group**

no neighbor *peer-group-name* **peer-group**

Syntax Description

peer-group-name	Name of the BGP peer group.

Defaults

There is no BGP peer group.

Command Modes

Address family configuration (config-router-af)
Router configuration (config-router)

Command History

Release	Modification
11.0	This command was introduced.
11.1(20)CC	The **nlri unicast**, **nlri multicast**, and **nlri unicast multicast** keywords were added.
12.0(2)S	The **nlri unicast**, **nlri multicast**, and **nlri unicast multicast** keywords were added.
12.0(7)T	The **nlri unicast**, **nlri multicast**, and **nlri unicast multicast** keywords were removed. Address family configuration mode was added.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
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

Often in a BGP or multiprotocol BGP speaker, many neighbors are configured with the same update policies (that is, same outbound route maps, distribute lists, filter lists, update source, and so on). Neighbors with the same update policies can be grouped into peer groups to simplify configuration and make update calculation more efficient.

Note Peer group members can span multiple logical IP subnets, and can transmit, or pass along, routes from one peer group member to another.

Once a peer group is created with the **neighbor peer-group** command, it can be configured with the **neighbor** commands. By default, members of the peer group inherit all the configuration options of the peer group. Members also can be configured to override the options that do not affect outbound updates.

All the peer group members will inherit the current configuration as well as changes made to the peer group. Peer group members will always inherit the following configuration options by default:

- remote-as (if configured)
- version
- update-source
- outbound route-maps
- outbound filter-lists
- outbound distribute-lists
- minimum-advertisement-interval
- next-hop-self

If a peer group is not configured with a remote-as option, the members can be configured with the **neighbor** {*ip-address* | *peer-group-name*} **remote-as** command. This command allows you to create peer groups containing external BGP (eBGP) neighbors.

Examples

The following example configurations show how to create these types of neighbor peer group:

- internal Border Gateway Protocol (iBGP) peer group
- eBGP peer group
- Multiprotocol BGP peer group

iBGP Peer Group

In the following example, the peer group named internal configures the members of the peer group to be iBGP neighbors. By definition, this is an iBGP peer group because the **router bgp** command and the **neighbor remote-as** command indicate the same autonomous system (in this case, autonomous system 100). All the peer group members use loopback 0 as the update source and use set-med as the outbound route map. The **neighbor internal filter-list 2 in** command shows that, except for 172.16.232.55, all the neighbors have filter list 2 as the inbound filter list.

```
router bgp 100
 neighbor internal peer-group
 neighbor internal remote-as 100
 neighbor internal update-source loopback 0
 neighbor internal route-map set-med out
 neighbor internal filter-list 1 out
 neighbor internal filter-list 2 in
 neighbor 172.16.232.53 peer-group internal
 neighbor 172.16.232.54 peer-group internal
 neighbor 172.16.232.55 peer-group internal
 neighbor 172.16.232.55 filter-list 3 in
```

eBGP Peer Group

The following example defines the peer group named external-peers without the **neighbor remote-as** command. By definition, this is an eBGP peer group because each individual member of the peer group is configured with its respective autonomous system number separately. Thus the peer group consists of

members from autonomous systems 200, 300, and 400. All the peer group members have the set-metric route map as an outbound route map and filter list 99 as an outbound filter list. Except for neighbor 172.16.232.110, all of them have 101 as the inbound filter list.

```
router bgp 100
 neighbor external-peers peer-group
 neighbor external-peers route-map set-metric out
 neighbor external-peers filter-list 99 out
 neighbor external-peers filter-list 101 in
 neighbor 172.16.232.90 remote-as 200
 neighbor 172.16.232.90 peer-group external-peers
 neighbor 172.16.232.100 remote-as 300
 neighbor 172.16.232.100 peer-group external-peers
 neighbor 172.16.232.110 remote-as 400
 neighbor 172.16.232.110 peer-group external-peers
 neighbor 172.16.232.110 filter-list 400 in
```

Multiprotocol BGP Peer Group

In the following example, all members of the peer group are multicast-capable:

```
router bgp 100
neighbor 10.1.1.1 remote-as 1
neighbor 172.16.2.2 remote-as 2
address-family ipv4 multicast
 neighbor mygroup peer-group
 neighbor 10.1.1.1 peer-group mygroup
 neighbor 172.16.2.2 peer-group mygroup
 neighbor 10.1.1.1 activate
 neighbor 172.16.2.2 activate
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
clear ip bgp peer-group	Removes all the members of a BGP peer group.
show ip bgp peer-group	Displays information about BGP peer groups.

neighbor remote-as

To add an entry to the BGP or multiprotocol BGP neighbor table, use the **neighbor remote-as** command in router configuration mode. To remove an entry from the table, use the **no** form of this command.

neighbor {*ip-address* | *ipv6-address*[**%**] | *peer-group-name*} **remote-as** *autonomous-system-number* [**alternate-as** *autonomous-system-number ...*]

no neighbor *{ip-address* | *ipv6-address*[**%**] | *peer-group-name*} **remote-as** *autonomous-system-number* [**alternate-as** *autonomous-system-number ...*]

Syntax Description

ip-address	IP address of the neighbor.
ipv6-address	IPv6 address of the neighbor.
%	(Optional) IPv6 link-local address identifier. This keyword needs to be added whenever a link-local IPv6 address is used outside the context of its interface.
peer-group-name	Name of a BGP peer group.
autonomous-system-number	Number of an autonomous system to which the neighbor belongs in the range from 1 to 65535. • In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, 4-byte autonomous system numbers are supported in the range from 65536 to 4294967295 in asplain notation and in the range from 1.0 to 65535.65535 in asdot notation. • In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, 4-byte autonomous system numbers are supported in the range from 1.0 to 65535.65535 in asdot notation only. For more details about autonomous system number formats, see the **router bgp** command. When used with the **alternate-as** keyword, up to five autonomous system numbers may be entered.
alternate-as	(Optional) Specifies an alternate autonomous system in which a potential dynamic neighbor can be identified. Up to five autonomous system numbers may be entered when this keyword is specified.

Command Default

There are no BGP or multiprotocol BGP neighbor peers.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
10.0	This command was introduced.
11.0	The *peer-group-name* argument was added.

Release	Modification
11.1(20)CC	The **nlri unicast**, **nlri multicast**, and **nlri unicast multicast** keywords were added.
12.0(7)T	The **nlri unicast**, **nlri multicast**, and **nlri unicast multicast** keywords were removed.
12.2(4)T	Support for the IPv6 address family was added.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was modified. The **%** keyword was added.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH. The **alternate-as** keyword was added to support BGP dynamic neighbors.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
12.0(32)S12	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(24)T	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.3	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SXI1	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
12.2(33)SRE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.

Usage Guidelines

Specifying a neighbor with an autonomous system number that matches the autonomous system number specified in the **router bgp** global configuration command identifies the neighbor as internal to the local autonomous system. Otherwise, the neighbor is considered external.

If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command.

By default, neighbors that are defined using the **neighbor remote-as** command in router configuration mode exchange only unicast address prefixes. To exchange other address prefix types, such as multicast and Virtual Private Network (VPN) Version 4, neighbors must also be activated in the appropriate address family configuration mode.

Use the **alternate-as** keyword introduced in Cisco IOS Release 12.2(33)SXH to specify up to five alternate autonomous systems in which a dynamic BGP neighbor may be identified. BGP dynamic neighbor support allows BGP peering to a group of remote neighbors that are defined by a range of IP addresses. BGP dynamic neighbors are configured using a range of IP addresses and BGP peer groups. After a subnet range is configured and associated with a BGP peer group using the **bgp listen** command and a TCP session is initiated for an IP address in the subnet range, a new BGP neighbor is dynamically created as a member of that group. The new BGP neighbor will inherit any configuration or templates for the group.

The **%** keyword is used whenever link-local IPv6 addresses are used outside the context of their interfaces. This keyword does not need to be used for non-link-local IPv6 addresses.

In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, the Cisco implementation of 4-byte autonomous system numbers uses asplain—65538 for example—as the default regular expression match and output display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain format and the asdot format as described in RFC 5396. To change the default regular expression match and output display of 4-byte autonomous system numbers to asdot format, use the **bgp asnotation dot** command followed by the **clear ip bgp *** command to perform a hard reset of all current BGP sessions.

In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, the Cisco implementation of 4-byte autonomous system numbers uses asdot—1.2 for example—as the only configuration format, regular expression match, and output display, with no asplain support.

Note In Cisco IOS releases that include 4-byte ASN support, command accounting and command authorization that include a 4-byte ASN number are sent in the asplain notation irrespective of the format that is used on the command-line interface.

To ensure a smooth transition, we recommend that all BGP speakers within an autonomous system that is identified using a 4-byte autonomous system number, be upgraded to support 4-byte autonomous system numbers.

Examples

The following example specifies that a router at the address 10.108.1.2 is an internal BGP (iBGP) neighbor in autonomous system number 65200:

```
router bgp 65200
 network 10.108.0.0
 neighbor 10.108.1.2 remote-as 65200
```

The following example specifies that a router at the IPv6 address 2001:0DB8:1:1000::72a is an external BGP (eBGP) neighbor in autonomous system number 65001:

```
router bgp 65300
 address-family ipv6 vrf site1
 neighbor 2001:0DB8:1:1000::72a remote-as 65001
```

The following example assigns a BGP router to autonomous system 65400, and two networks are listed as originating in the autonomous system. Then the addresses of three remote routers (and their autonomous systems) are listed. The router being configured will share information about networks 10.108.0.0 and 192.168.7.0 with the neighbor routers. The first router is a remote router in a different autonomous system from the router on which this configuration is entered (an eBGP neighbor); the second **neighbor remote-as** command shows an internal BGP neighbor (with the same autonomous

system number) at address 10.108.234.2; and the last **neighbor remote-as** command specifies a neighbor on a different network from the router on which this configuration is entered (also an eBGP neighbor).

```
router bgp 65400
 network 10.108.0.0
 network 192.168.7.0
 neighbor 10.108.200.1 remote-as 65200
 neighbor 10.108.234.2 remote-as 65400
 neighbor 172.29.64.19 remote-as 65300
```

The following example configures neighbor 10.108.1.1 in autonomous system 65001 to exchange only multicast routes:

```
router bgp 65001
 neighbor 10.108.1.1 remote-as 65001
 neighbor 172.31 1.2 remote-as 65001
 neighbor 172.16.2.2 remote-as 65002
 address-family ipv4 multicast
  neighbor 10.108.1.1 activate
  neighbor 172.31 1.2 activate
  neighbor 172.16.2.2 activate
  exit-address-family
```

The following example configures neighbor 10.108.1.1 in autonomous system 65001 to exchange only unicast routes:

```
router bgp 65001
 neighbor 10.108.1.1 remote-as 65001
 neighbor 172.31 1.2 remote-as 65001
 neighbor 172.16.2.2 remote-as 65002
```

The following example, configurable only in Cisco IOS Release 12.2(33)SXH and later releases, configures a subnet range of 192.168.0.0/16 and associates this listen range with a BGP peer group. Note that the listen range peer group that is configured for the BGP dynamic neighbor feature can be activated in the IPv4 address family using the **neighbor activate** command. After the initial configuration on Router 1, when Router 2 starts a BGP router session and adds Router 1 to its BGP neighbor table, a TCP session is initiated, and Router 1 creates a new BGP neighbor dynamically because the IP address of the new neighbor is within the listen range subnet.

Router 1

```
enable
configure terminal
router bgp 45000
 bgp log-neighbor-changes
 neighbor group192 peer-group
 bgp listen range 192.168.0.0/16 peer-group group192
 neighbor group192 remote-as 40000 alternate-as 50000
 address-family ipv4 unicast
 neighbor group192 activate
 end
```

Router 2

```
enable
configure terminal
router bgp 50000
 neighbor 192.168.3.1 remote-as 45000
 exit
```

If the **show ip bgp summary** command is now entered on Router 1, the output shows the dynamically created BGP neighbor, 192.168.3.2.

```
Router1# show ip bgp summary

BGP router identifier 192.168.3.1, local AS number 45000
BGP table version is 1, main routing table version 1

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
*192.168.3.2    4 50000       2       2        0    0    0 00:00:37        0
* Dynamically created based on a listen range command
Dynamically created neighbors: 1/(200 max), Subnet ranges: 1

BGP peergroup group192 listen range group members:
  192.168.0.0/16
```

The following example configures a BGP process for autonomous system 65538 and configures two external BGP neighbors in different autonomous systems using 4-byte autonomous system numbers in asplain format. This example is supported only on Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, or later releases.

```
router bgp 65538
 neighbor 192.168.1.2 remote-as 65536
 neighbor 192.168.3.2 remote-as 65550
 neighbor 192.168.3.2 description finance
 !
 address-family ipv4
  neighbor 192.168.1.2 activate
  neighbor 192.168.3.2 activate
  no auto-summary
  no synchronization
  network 172.17.1.0 mask 255.255.255.0
  exit-address-family
```

The following example configures a BGP process for autonomous system 1.2 and configures two external BGP neighbors in different autonomous systems using 4-byte autonomous system numbers in asdot format. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(32)S12, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, 12.4(24)T, Cisco IOS XE Release 2.3, or a later release.

```
router bgp 1.2
 neighbor 192.168.1.2 remote-as 1.0
 neighbor 192.168.3.2 remote-as 1.14
 neighbor 192.168.3.2 description finance
 !
 address-family ipv4
  neighbor 192.168.1.2 activate
  neighbor 192.168.3.2 activate
  no auto-summary
  no synchronization
  network 172.17.1.0 mask 255.255.255.0
  exit-address-family
```

Related Commands

Command	Description
bgp asnotation dot	Changes the default display and the regular expression match format of BGP 4-byte autonomous system numbers from asplain (decimal values) to dot notation.
bgp listen	Associates a subnet range with a BGP peer group and activates the BGP dynamic neighbors feature.

neighbor peer-group	Creates a BGP peer group.
router bgp	Configures the BGP routing process.

neighbor route-map

To apply a route map to incoming or outgoing routes, use the **neighbor route-map** command in address family or router configuration mode. To remove a route map, use the **no** form of this command.

neighbor {*ip-address* | *peer-group-name* | *ipv6-address* [**%**]} **route-map** *map-name* {**in** | **out**}

no neighbor {*ip-address* | *peer-group-name* | *ipv6-address* [**%**]} **route-map** *map-name* {**in** | **out**}

Syntax Description

ip-address	IP address of the neighbor.
peer-group-name	Name of a BGP or multiprotocol BGP peer group.
ipv6-address	IPv6 address of the neighbor.
%	(Optional) IPv6 link-local address identifier. This keyword needs to be added whenever a link-local IPv6 address is used outside the context of its interface.
map-name	Name of a route map.
in	Applies route map to incoming routes.
out	Applies route map to outgoing routes.

Command Default

No route maps are applied to a peer.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
10.0	This command was introduced.
12.0(7)T	Address family configuration mode was added.
12.2(4)T	Support for IPv6 was added.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	The **%** keyword was added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

When specified in address family configuration mode, this command applies a route map to that particular address family only. When specified in router configuration mode, this command applies a route map to IPv4 or IPv6 unicast routes only.

If an outbound route map is specified, it is proper behavior to only advertise routes that match at least one section of the route map.

If you specify a BGP or multiprotocol BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command. Specifying the command for a neighbor overrides the inbound policy that is inherited from the peer group.

The **%** keyword is used whenever link-local IPv6 addresses are used outside the context of their interfaces. This keyword does not need to be used for non-link-local IPv6 addresses.

Examples

The following router configuration mode example applies a route map named internal-map to a BGP incoming route from 172.16.70.24:

```
router bgp 5
 neighbor 172.16.70.24 route-map internal-map in

route-map internal-map
 match as-path 1
 set local-preference 100
```

The following address family configuration mode example applies a route map named internal-map to a multiprotocol BGP incoming route from 172.16.70.24:

```
router bgp 5
address-family ipv4 multicast
 neighbor 172.16.70.24 route-map internal-map in

route-map internal-map
 match as-path 1
 set local-preference 100
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IP Version 4 address prefixes.
address-family ipv6	Enters address family configuration mode for configuring routing sessions such as BGP that use standard IPv6 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPN Version 4 address prefixes.
address-family vpnv6	Places the router in address family configuration mode for configuring routing sessions that use standard VPNv6 address prefixes.
neighbor remote-as	Creates a BGP peer group.

neighbor route-reflector-client

To configure the router as a BGP route reflector and configure the specified neighbor as its client, use the **neighbor route-reflector-client** command in address family or router configuration mode. To indicate that the neighbor is not a client, use the **no** form of this command.

neighbor {*ip-address* | *ipv6-address* | *peer-group-name*} **route-reflector-client**

no neighbor {*ip-address* | *ipv6-address* | *peer-group-name*} **route-reflector-client**

Syntax Description

ip-address	IP address of the BGP neighbor being identified as a client.
ipv6-address	IPv6 address of the BGP neighbor being identified as a client.
peer-group-name	Name of a BGP peer group.

Command Default

There is no route reflector in the autonomous system.

Command Modes

Address family configuration (config-router-af)
Router configuration (config-router)

Command History

Release	Modification
11.1	This command was introduced.
12.0(7)T	Address family configuration mode was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	The *ipv6-address* and *peer-group-name* arguments were 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.
Cisco IOS XE Release 3.1S	This command was updated. It was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

By default, all internal BGP (iBGP) speakers in an autonomous system must be fully meshed, and neighbors do not readvertise iBGP learned routes to neighbors, thus preventing a routing information loop. When all the clients are disabled, the local router is no longer a route reflector.

If you use route reflectors, all iBGP speakers need not be fully meshed. In the route reflector model, an Interior BGP peer is configured to be a *route reflector* responsible for passing iBGP learned routes to iBGP neighbors. This scheme eliminates the need for each router to talk to every other router.

Use the **neighbor route-reflector-client** command to configure the local router as the route reflector and the specified neighbor as one of its clients. All the neighbors configured with this command will be members of the client group and the remaining iBGP peers will be members of the nonclient group for the local route reflector.

The **bgp client-to-client reflection** command controls client-to-client reflection.

Examples

In the following router configuration mode example, the local router is a route reflector. It passes learned iBGP routes to the neighbor at 172.16.70.24.

```
router bgp 5
 neighbor 172.16.70.24 route-reflector-client
```

In the following address family configuration mode example, the local router is a route reflector. It passes learned iBGP routes to the neighbor at 172.16.70.24.

```
router bgp 5
address-family ipv4 unicast
 neighbor 172.16.70.24 route-reflector-client
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IP Version 4 address prefixes.
address-family ipv6	Enters address family configuration mode for configuring routing sessions such as BGP that use standard IPv6 address prefixes.
address-family vpnv6	Places the router in address family configuration mode for configuring routing sessions such as BGP that use standard VPNv6 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPN Version 4 address prefixes.
address-family vpnv6	Places the router in address family configuration mode for configuring routing sessions such as BGP that use standard VPNv6 address prefixes.
bgp client-to-client reflection	Restores route reflection from a BGP route reflector to clients.
bgp cluster-id	Configures the cluster ID if the BGP cluster has more than one route reflector.
neighbor route-reflector-client	Configures the router as a BGP route reflector and configures the specified neighbor as its client.
show bgp ipv6	Displays entries in the IPv6 BGP routing table.
show ip bgp	Displays entries in the BGP routing table.

neighbor send-community

To specify that a communities attribute should be sent to a BGP neighbor, use the **neighbor send-community** command in address family or router configuration mode. To remove the entry, use the **no** form of this command.

neighbor {*ip-address* | *ipv6-address* | *peer-group-name*} **send-community** [**both** | **standard** | **extended**]

no neighbor {*ip-address* | *ipv6-address* | *peer-group-name*} **send-community**

Syntax Description

ip-address	IP address of the neighbor.
ipv6-address	IPv6 address of the neighbor.
peer-group-name	Name of a BGP peer group.
both	(Optional) Specifies that both standard and extended communities will be sent.
standard	(Optional) Specifies that only standard communities will be sent.
extended	(Optional) Specifies that only extended communities will be sent.

Command Default

No communities attribute is sent to any neighbor.

Command Modes

Address family configuration (config-router-af)
Router configuration (config-router)

Command History

Release	Modification
10.3	This command was introduced.
11.0	The *peer-group-name* argument was added.
12.0(7)T	Address family configuration mode was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	The *ipv6-address* argument 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.

Usage Guidelines

If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command.

Examples

In the following router configuration mode example, the router belongs to autonomous system 109 and is configured to send the communities attribute to its neighbor at IP address 172.16.70.23:

```
router bgp 109
 neighbor 172.16.70.23 send-community
```

In the following address family configuration mode example, the router belongs to autonomous system 109 and is configured to send the communities attribute to its neighbor at IP address 172.16.70.23:

```
router bgp 109
address-family ipv4 multicast
 neighbor 172.16.70.23 send-community
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IP Version 4 address prefixes.
address-family ipv6	Places the router in address family configuration mode for configuring routing sessions such as BGP that use standard IPv6 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPN Version 4 address prefixes.
address-family vpnv6	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard VPNv6 address prefixes.
match community	Matches a BGP community.
neighbor remote-as	Creates a BGP peer group.
set community	Sets the BGP communities attribute.

neighbor send-label

To enable a Border Gateway Protocol (BGP) router to send Multiprotocol Label Switching (MPLS) labels with BGP routes to a neighboring BGP router, use the **neighbor send-label** command in address family configuration mode or router configuration mode. To disable this feature, use the **no** form of this command.

neighbor {*ip-address* | *ipv6-address* | *peer-group-name*} **send-label** [**explicit-null**]

neighbor {*ip-address* | *ipv6-address* | *peer-group-name*} **send-label** [**explicit-null**]

Syntax Description

ip-address	IP address of the neighboring router.
ipv6-address	IPv6 address of the neighboring router.
peer-group-name	Name of a BGP peer group.
send-label	Sends Network Layer Reachability Information (NLRI) and MPLS labels to this peer.
explicit-null	(Optional) Advertises the Explicit Null label.

Command Default

BGP routers distribute only BGP routes.

Command Modes

Address family configuration (config-router-af)
Router configuration (config-router)

Command History

Release	Modification
12.0(21)ST	This command was introduced.
12.0(22)S	This command was modified. The *ipv6-address* argument was added.
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.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
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.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

The **neighbor send-label** command enables a router to use BGP to distribute MPLS labels along with IPv4 routes to a peer router. You must issue this command on both the local and the neighboring router.

This command has the following restrictions:

- If a BGP session is running when you issue the **neighbor send-label** command, the BGP session flaps immediately after the command is issued.

- In router configuration mode, only IPv4 addresses are distributed.

Use the **neighbor send-label** command in address family configuration mode, to bind and advertise IPv6 prefix MPLS labels. Using this command in conjunction with the **mpls ipv6 source-interface** global configuration command allows IPv6 traffic to run over an IPv4 MPLS network without any software or hardware configuration changes in the backbone. Edge routers configured to run both IPv4 and IPv6 traffic forward IPv6 traffic using MPLS and multiprotocol internal BGP (MP-iBGP).

Cisco IOS software installs /32 routes for directly connected external BGP (eBGP) peers when the BGP session for such a peer comes up. The /32 routes are installed only when MPLS labels are exchanged between such peers. Directly connected eBGP peers exchange MPLS labels for:

- IP address families (IPv4 and IPv6) with the **neighbor send-label** command enabled for the peers
- VPN address families (VPNv4 and VPNv6)

A single BGP session can include multiple address families. If one of the families exchanges MPLS labels, the /32 neighbor route is installed for the connected peer.

Examples

The following example shows how to enable a router in autonomous system 65000 to send MPLS labels with BGP routes to the neighboring BGP router at 192.168.0.1:

```
Router(config)# router bgp 65000
Router(config-router)# neighbor 192.168.0.1 remote-as 65001
Router(config-router)# neighbor 192.168.0.1 send-label
```

The following example shows how to enable a router in the autonomous system 65000 to bind and advertise IPv6 prefix MPLS labels and send the labels with BGP routes to the neighboring BGP router at 192.168.99.70:

```
Router(config)# router bgp 65000
Router(config-router)# neighbor 192.168.99.70 remote-as 65000
Router(config-router)# address-family ipv6
Router(config-router-af)# neighbor 192.168.99.70 activate
Router(config-router-af)# neighbor 192.168.99.70 send-label
```

Related Commands

Command	Description
address-family ipv6	Enters address family configuration mode for configuring routing sessions such as BGP that use standard IPv6 address prefixes.
neighbor activate	Enables the exchange of information with a neighboring router.
neighbor remote-as	Adds an entry to the BGP or multiprotocol BGP neighbor table.
mpls ipv6 source-interface	Specifies an IPv6 address of an interface to be used as the source address for locally generated IPv6 packets to be sent over an MPLS network.

neighbor translate-update

To generate multiprotocol IPv6 Border Gateway Protocol (BGP) updates that correspond to unicast IPv6 updates received from a peer, use the **neighbor translate-update** command in address family or router configuration mode. To return to default values, use the **no** form of the command.

neighbor *ipv6-address* **translate-update ipv6 multicast** [**unicast**]

no neighbor *ipv6-address* **translate-update ipv6 multicast** [**unicast**]

Syntax Description

ipv6-address	Resets the TCP connection to the specified IPv6 BGP neighbor and removes all routes learned from the connection from the BGP table. 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 multicast	Specifies IPv6 multicast address prefixes.
unicast	(Optional) Specifies IPv6 unicast address prefixes.

Command Default

No BGP updates for unicast IPv6 are updated

Command Modes

Address family configuration
Router configuration

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
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.
12.2(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 introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The multicast BGP (MBGP) translate-update feature generally is used in an MBGP-capable router that peers with a customer site that has a router that is only BGP capable; the customer site has not or cannot upgrade the router to an MBGP-capable image. Because the customer site cannot originate MBGP advertisements, the router with which it peers will translate the BGP prefixes into MBGP prefixes, which are used for multicast-source Reverse Path Forwarding (RPF) lookup.

Examples

The following example generates multiprotocol IPv6 BGP updates that correspond to unicast IPv6 updates received from peer at address 7000::2:

```
neighbor 7000::2 translate-update ipv6 multicast
```

neighbor update-source

To have the Cisco IOS software allow Border Gateway Protocol (BGP) sessions to use any operational interface for TCP connections, use the **neighbor update-source** command in router configuration mode. To restore the interface assignment to the closest interface, which is called the best local address, use the **no** form of this command.

neighbor {*ip-address* | *ipv6-address*[**%**] | *peer-group-name*} **update-source** *interface-type interface-number*

no neighbor {*ip-address* | *ipv6-address*[**%**] | *peer-group-name*} **update-source** *interface-type interface-number*

Syntax Description

ip-address	IPv4 address of the BGP-speaking neighbor.
ipv6-address	IPv6 address of the BGP-speaking neighbor.
%	(Optional) IPv6 link-local address identifier. This keyword needs to be added whenever a link-local IPv6 address is used outside the context of its interface.
peer-group-name	Name of a BGP peer group.
interface-type	Interface type.
interface-number	Interface number.

Command Default

Best local address

Command Modes

Router configuration (config-router)

Command History

Release	Modification
10.0	This command was introduced.
12.2(4)T	The *ipv6-address* argument was added.
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 Release 12.2(14)S.
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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	The **%** 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.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 series routers.

Usage Guidelines

This command can work in conjunction with the loopback interface feature described in the "Interface Configuration Overview" chapter of the *Cisco IOS Interface and Hardware Component Configuration Guide*.

If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command.

The **neighbor update-source** command must be used to enable IPv6 link-local peering for internal or external BGP sessions.

The **%** keyword is used whenever link-local IPv6 addresses are used outside the context of their interfaces and for these link-local IPv6 addresses you must specify the interface they are on. The syntax becomes <IPv6 local-link address>%<interface name>, for example, FE80::1%Ethernet1/0. Note that the interface type and number must not contain any spaces, and be used in full-length form because name shortening is not supported in this situation. The % keyword and subsequent interface syntax is not used for non-link-local IPv6 addresses.

Examples

The following example sources BGP TCP connections for the specified neighbor with the IP address of the loopback interface rather than the best local address:

```
router bgp 65000
 network 172.16.0.0
 neighbor 172.16.2.3 remote-as 110
 neighbor 172.16.2.3 update-source Loopback0
```

The following example sources IPv6 BGP TCP connections for the specified neighbor in autonomous system 65000 with the global IPv6 address of loopback interface 0 and the specified neighbor in autonomous system 65400 with the link-local IPv6 address of Fast Ethernet interface 0/0. Note that the link-local IPv6 address of FE80::2 is on Ethernet interface 1/0.

```
router bgp 65000
 neighbor 3ffe::3 remote-as 65000
 neighbor 3ffe::3 update-source Loopback0
 neighbor fe80::2%Ethernet1/0 remote-as 65400
 neighbor fe80::2%Ethernet1/0 update-source FastEthernet 0/0
 address-family ipv6
  neighbor 3ffe::3 activate
  neighbor fe80::2%Ethernet1/0 activate
  exit-address-family
```

Related Commands

Command	Description
neighbor activate	Enables the exchange of information with a BGP neighboring router.
neighbor remote-as	Adds an entry to the BGP or multiprotocol BGP neighbor table.

network (BGP and multiprotocol BGP)

To specify the networks to be advertised by the Border Gateway Protocol (BGP) and multiprotocol BGP routing processes, use the **network** command in address family or router configuration mode. To remove an entry from the routing table, use the **no** form of this command.

network {*network-number* [**mask** *network-mask*] | *nsap-prefix*} [**route-map** *map-tag*]

no network {*network-number* [**mask** *network-mask*] | *nsap-prefix*} [**route-map** *map-tag*]

Syntax Description

network-number	Network that BGP or multiprotocol BGP will advertise.
mask *network-mask*	(Optional) Network or subnetwork mask with mask address.
nsap-prefix	Network service access point (NSAP) prefix of the Connectionless Network Service (CLNS) network that BGP or multiprotocol BGP will advertise. This argument is used only under NSAP address family configuration mode.
route-map *map-tag*	(Optional) Identifier of a configured route map. The route map should be examined to filter the networks to be advertised. If not specified, all networks are advertised. If the keyword is specified, but no route map tags are listed, no networks will be advertised.

Command Default

No networks are specified.

Command Modes

Address family configuration (config-router-af)
Router configuration (config-router)

Command History

Release	Modification
10.0	This command was introduced.
12.0	The limit of 200 network commands per BGP router was removed.
11.1(20)CC	The **nlri unicast**, **nlri multicast**, and **nlri unicast multicast** keywords were added.
12.0(7)T	The **nlri unicast**, **nlri multicast**, and **nlri unicast multicast** keywords were removed. Address family configuration mode was added.
12.2(8)T	The *nsap-prefix* argument was added to address family configuration mode.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
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.
Cisco IOS XE 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

BGP and multiprotocol BGP networks can be learned from connected routes, from dynamic routing, and from static route sources.

The maximum number of **network** commands you can use is determined by the resources of the router, such as the configured NVRAM or RAM.

Examples

The following example sets up network 10.108.0.0 to be included in the BGP updates:

```
router bgp 65100
 network 10.108.0.0
```

The following example sets up network 10.108.0.0 to be included in the multiprotocol BGP updates:

```
router bgp 64800
address family ipv4 multicast
 network 10.108.0.0
```

The following example advertises NSAP prefix 49.6001 in the multiprotocol BGP updates:

```
router bgp 64500
 address-family nsap
  network 49.6001
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Enters the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IP Version 4 address prefixes.
address-family vpnv4	Enters the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
default-information originate (BGP)	Allows the redistribution of network 0.0.0.0 into BGP.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another.
router bgp	Configures the BGP routing process.

network (IPv6)

To configure the network source of the next hop to be used by the PE VPN, use the **network** command in router configuration mode. To disable the source, use the **no** form of this command.

network *ipv6-address*/*prefix-length*

no network *ipv6-address*/*prefix-length*

Syntax Description

ipv6-address	The IPv6 address to be used.
/*prefix-length*	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

Command Default

Next-hop network sources are not configured.

Command Modes

Address family configuration
Router configuration

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
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.
Cisco IOS XE Release 3.1S	This command was updated. It was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

The *ipv6-address* argument in this command configures the IPv6 network number.

Examples

The following example places the router in address family configuration mode and configures the network source to be used as the next hop:

```
Router(config)# router bgp 100
Router(config-router)# network 2001:DB8:100::1/128
```

Related Commands

Command	Description
address-family ipv6	Enters address family configuration mode for configuring routing sessions such as BGP that use standard IPv6 address prefixes.
address-family vpnv6	Places the router in address family configuration mode for configuring routing sessions that use standard VPNv6 address prefixes.

nis address

To specify the network information service (NIS) address of an IPv6 server to be sent to the client, use the **nis address** command in DHCP for IPv6 pool configuration mode. To remove the NIS address, use the **no** form of this command.

nis address *ipv6-address*

no nis address *ipv6-address*

Syntax Description

ipv6-address	The NIS address of an IPv6 server to be sent to the client.

Command Default

No NIS address is specified.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

The Dynamic Host Configuration Protocol (DHCP) for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The NIS server option provides a list of one or more IPv6 addresses of NIS servers available to send to the client. The client must view the list of NIS servers as an ordered list, and the server may list the NIS servers in the order of the server's preference.

The NIS server option code is 27. For more information on DHCP options and suboptions, see the "DHCPv6 Options" appendix in the *Network Registrar User's Guide*, Release 6.2.

Examples

The following example shows how to specify the NIS address of an IPv6 server:

```
nis address 23::1
```

Related Commands

Command	Description
import nis address	Imports the NIS server option to a DHCP for IPv6 client.
nis domain-name	Enables a server to convey a client's NIS domain name information to the client.

nis domain-name

To enable a server to convey a client's network information service (NIS) domain name information to the client, use the **nis domain-name** command in DHCP for IPv6 pool configuration mode. To remove the domain name, use the **no** form of this command.

nis domain-name *domain-name*

no nis domain-name *domain-name*

Syntax Description

domain-name	The domain name of an IPv6 server to be sent to the client.

Command Default

No NIS domain name is specified.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

The Dynamic Host Configuration Protocol (DHCP) for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The NIS domain name option provides a NIS domain name for the client. Use the **nis domain-name** command to specify the client's NIS domain name that the server sends to the client.

The NIS domain name option code is 29. For more information on DHCP options and suboptions, see the "DHCPv6 Options" appendix in the *Network Registrar User's Guide*, Release 6.2.

Examples

The following example shows how to enable the IPv6 server to specify the NIS domain name of a client:

```
nis domain-name cisco1.com
```

Related Commands

Command	Description
import nis domain	Imports the NIS domain name option to a DHCP for IPv6 client.
nis address	Specifies the NIS address of an IPv6 server to be sent to the client.

nisp address

To specify the network information service plus (NIS+) address of an IPv6 server to be sent to the client, use the **nisp address** command in DHCP for IPv6 pool configuration mode. To remove the NIS+ address, use the **no** form of the command.

nisp address *ipv6-address*

no nisp address *ipv6-address*

Syntax Description

ipv6-address	The NIS+ address of an IPv6 server to be sent to the client.

Command Default

No NIS+ address is specified.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

The Dynamic Host Configuration Protocol (DHCP) for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The NIS+ servers option provides a list of one or more IPv6 addresses of NIS+ servers available to send to the client. The client must view the list of NIS+ servers as an ordered list, and the server may list the NIS+ servers in the order of the server's preference.

The NIS+ servers option code is 28. For more information on DHCP options and suboptions, see the "DHCPv6 Options" appendix in the *Network Registrar User's Guide*, Release 6.2.

Examples

The following example shows how to specify the NIS+ address of an IPv6 server:

```
nisp address 33::1
```

Related Commands

Command	Description
import nisp address	Imports the NIS+ servers option to a DHCP for IPv6 client.
nisp domain-name	Enables a server to convey a client's NIS+ domain name information to the client.

nisp domain-name

To enable an IPv6 server to convey a client's network information service plus (NIS+) domain name information to the client, use the **nisp domain-name** command in DHCP for IPv6 pool configuration mode. To remove the domain name, use the **no** form of this command.

nisp domain-name *domain-name*

no nisp domain-name *domain-name*

Syntax Description

domain-name	The NIS+ domain name of an IPv6 server to be sent to the client.

Command Default

No NIS+ domain name is specified.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

The Dynamic Host Configuration Protocol (DHCP) for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The NIS+ domain name option provides a NIS+ domain name for the client. Use the **nisp domain-name** command to enable a server to send the client its NIS+ domain name information.

The NIS+ domain name option code is 30. For more information on DHCP options and suboptions, see the "DHCPv6 Options" appendix in the *Network Registrar User's Guide*, Release 6.2.

Examples

The following example shows how to enable the IPv6 server to specify the NIS+ domain name of a client:

```
nisp domain-name cisco1.com
```

Related Commands

Command	Description
import nisp domain	Imports the NIS+ domain name option to a DHCP for IPv6 client.
nisp address	Specifies the NIS+ address of an IPv6 server to be sent to the client.

ntp access-group

To control access to the Network Time Protocol (NTP) services on the system, use the **ntp access-group** command in global configuration mode. To remove access control to the NTP services, use the **no** form of this command.

ntp access-group {**peer** | **query-only** | **serve** | **serve-only**} {*access-list-number* | *access-list-number-expanded* | *access-list-name*} [**kod**]

no ntp [**access-group** {**peer** | **query-only** | **serve** | **serve-only**} {*access-list-number* | *access-list-number-expanded* | *access-list-name*}]

Syntax Description

peer	Allows time requests and NTP control queries and allows the system to synchronize to the remote system.
query-only	Allows only NTP control queries. See RFC 1305 (NTP version 3).
serve	Allows time requests and NTP control queries, but does not allow the system to synchronize to the remote system.
serve-only	Allows only time requests. **Note** You must configure the **ntp server** *ip-address* command before using the **serve-only** keyword.
access-list-number	Number (from 1 to 99) of a standard IPv4 access list.
access-list-number-expanded	Number (from 1300 to 1999) of an expanded range IPv4 access list.
access-list-name	Name of an access list.
kod	(Optional) Sends the "Kiss-o-Death" (KOD) packet to any host that tries to send a packet that is not compliant with the access-group policy.

Command Default

By default, there is no access control. Full access is granted to all systems.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.4(15)T	This command was modified in a release earlier than Cisco IOS Release 12.4(15)T. The *access-list-number-expanded* argument 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(20)T	This command was modified. The *access-list-name* argument and **kod** keyword were added. Support for IPv6 was added.

Release	Modification
12.2(33)SXJ	This command was modified. The *access-list-name* argument and **kod** keyword were added. Support for IPv6 was added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

The access group options are scanned in the following order from the least restrictive to most restrictive:

1. **peer**
2. **query-only**
3. **serve**
4. **serve-only**

Access is granted for the first match that is found. If no access groups are specified, all access is granted to all sources. If you specify any access groups, only the specified access is granted. This facility provides minimal security for the time services of the system. However, it can be circumvented by a determined programmer. If tighter security is desired, use the NTP authentication facility.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp access-group** command, the NTP service is activated (if it has not already been activated) and access control to NTP services is configured simultaneously.

When you enter the **no ntp access-group** command, only access control to NTP services is removed. The NTP service itself remains active, along with any other previously configured NTP functions.

To disable the NTP service on a device, use the **no ntp** command without any keywords in global configuration mode. For example, if you want to remove not only the access control to NTP services, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

Examples

The following example shows how to configure a system to allow itself to be synchronized by a peer from access list 99. However, the system restricts access to allow only time requests from access list 42.

```
Router(config)# ntp access-group peer 99
Router(config)# ntp access-group serve-only 42
```

In the following IPv6 example, a KOD packet is sent to any host that tries to send a packet that is not compliant with the access-group policy:

```
Router(config)# ntp access-group serve acl1 kod
```

The following example shows how to remove all the configured NTP options and disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
access-list	Configures the access list mechanism for filtering frames by protocol type or vendor code.
ntp server	Allows the software clock to be synchronized by a time server.

ntp authenticate

To enable Network Time Protocol (NTP) authentication, use the **ntp authenticate** command in global configuration mode. To disable the function, use the **no** form of this command.

ntp authenticate

no ntp [**authenticate**]

Syntax Description

This command has no arguments or keywords.

Command Default

By default, NTP authentication is not enabled.

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.
12.4(20)T	This command was modified. Support for NTPv4 and IPv6 was added.
12.2(33)SXJ	This command was modified. Support for NTPv4 and IPv6 was added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

Use this command if you want to authenticate NTP. If this command is specified, the system will not synchronize to another system unless it carries one of the authentication keys specified in the **ntp trusted-key** global configuration command.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp authenticate** command, the NTP service is activated (if it has not already been activated) and NTP authentication is enabled simultaneously.

In the **no** form of any **ntp** command, all the keywords are optional. When you enter the **no ntp authenticate** command, only the NTP authentication is removed from the NTP service. The NTP service itself remains active, along with any other functions you that previously configured.

To disable the NTP service on a device, you must enter the **no ntp** command without any keywords in global configuration mode. For example, if you previously issued the **ntp authenticate** command and you now want to disable not only the authentication, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

Examples

The following example shows how to configure the system to synchronize only to systems that provide the authentication key 42 in their NTP packets:

```
Router(config)# ntp authenticate
Router(config)# ntp authentication-key 42 md5 aNiceKey
Router(config)# ntp trusted-key 42
```

The following example shows how to remove all the configured NTP options and disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
ntp authentication-key	Defines an authentication key for NTP.
ntp trusted-key	Authenticates the identity of a system to which NTP will synchronize.

ntp authentication-key

To define an authentication key for Network Time Protocol (NTP), use the **ntp authentication-key** command in global configuration mode. To remove the authentication key for NTP, use the **no** form of this command.

ntp authentication-key *number* **md5** *key* [*encryption-type*]

no ntp [**authentication-key** *number*]

Syntax Description

number	Key number from 1 to 4294967295.
md5	Specifies the authentication key. Message authentication support is provided using the message digest 5 (MD5) algorithm. The key type **md5** is the only key type supported.
key	Character string of up to 32 characters that is the value of the MD5 key. **Note** In auto secure mode, an error is displayed on the console and the authentication key is not configured if the character string length exceeds 32.
encryption-type	(Optional) Authentication key encryption type. Range: 0 to 4294967295.

Command Default

No authentication key is defined for NTP.

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.
12.4(20)T	This command was modified. Support for NTPv4 and IPv6 was added.
12.2(33)SXJ	This command was modified. Support for NTPv4 and IPv6 was added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

Use this command to define authentication keys for use with other NTP commands in order to provide a higher degree of security.

Note When this command is written to NVRAM, the key is encrypted so that it is not displayed in the configuration.

When you configure the authentication key using the **ntp authentication-key** command or using the **auto secure ntp** command, if the length of the MD5 key exceeds 32 characters, an error message is displayed.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp authentication-key** command, the NTP service is activated (if it has not already been activated) and the NTP authentication key is defined simultaneously.

When you enter the **no ntp authentication-key** command, only the NTP authentication key is removed from the NTP service. The NTP service itself remains active, along with any other previously configured NTP functions.

Note If a specific authentication key configuration is removed, the NTP process is not stopped until all the authentication key configurations are removed.

To disable the NTP service on a device, use the **no ntp** command without any keywords in global configuration mode. For example, if you want to remove not only the access control to NTP services, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

Examples

The following example shows how to configure the system to synchronize only to systems providing the authentication key 42 in their NTP packets:

```
Router(config)# ntp authenticate
Router(config)# ntp authentication-key 42 md5 aNiceKey
Router(config)# ntp trusted-key 42
```

The following example shows how to remove all the configured NTP options and disable the NTP server:

```
Router(config)# no ntp
```

The following example shows the error message displayed when the authentication key character string length exceeds 32:

```
Router(config)# ntp authentication-key 23 md5 11111111111111111111111111111111
%NTP: Key too long
```

Related Commands

Command	Description
auto secure	Secures the management and forwarding planes of the router.
ntp authenticate	Enables NTP authentication.
ntp peer	Configures the software clock to synchronize a peer or to be synchronized by a peer.
ntp server	Allows the software clock to be synchronized by a time server.
ntp trusted-key	Authenticates the identity of a system to which NTP will synchronize.

ntp broadcast client

To configure a device to receive Network Time Protocol (NTP) broadcast messages on a specified interface, use the **ntp broadcast client** command in interface configuration mode. To disable this capability, use the **no** form of this command.

ntp broadcast client [**novolley**]

no ntp [**broadcast** [**client**]]

Syntax Description

novolley	(Optional) Disables any messages sent to the broadcast server. Avoids the propagation delay measurement phase and directly uses a preconfigured value instead when used in conjunction with the **ntp broadcastdelay** command. **Note** Public key authentication does not work without the volley.

Command Default

By default, an interface is not configured to receive NTP broadcast messages.

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.
12.4(20)T	This command was modified. Support for NTPv4 and IPv6 was added. The **novolley** keyword was added.
12.2(33)SXJ	This command was modified. Support for NTPv4 and IPv6 was added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

Use this command to allow the system to listen to broadcast packets on an interface-by-interface basis.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp broadcast client** command, the NTP service is activated (if it has not already been activated) and the device is configured to receive NTP broadcast packets on a specified interface simultaneously.

In the **no** form of any **ntp** command, all the keywords are optional. When you enter the **no ntp broadcast client** command, only the broadcast client configuration is removed from the NTP service. The NTP service itself remains active, along with any other functions that you previously configured.

To disable the NTP service on a device, you must enter the **no ntp** command without any keywords. For example, if you previously issued the **ntp broadcast client** command and you now want to remove not only the broadcast client capability, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

In IPv6 configuration, the **ntp broadcastdelay** command is used when the **ntp broadcast client** or **ntp multicast client** command is configured with the **novolley** keyword.

Examples

In the following example, the system is configured to receive (listen to) NTP broadcasts on Ethernet interface 1:

```
Router(config)# interface ethernet 1
Router(config-if)# ntp broadcast client
```

The following example shows how to remove all the configured NTP options and disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
ntp broadcastdelay	Sets the estimated round-trip delay between the system and an NTP broadcast server.
ntp multicast client	Configures the system to receive NTP multicast packets on a specified interface.

ntp broadcastdelay

To set the estimated round-trip delay between the Cisco IOS software and a Network Time Protocol (NTP) broadcast server, use the **ntp broadcastdelay** command in global configuration mode. To revert to the default value, use the **no** form of this command.

ntp broadcastdelay *microseconds*

no ntp [**broadcastdelay**]

Syntax Description

microseconds	Estimated round-trip time (in microseconds) for NTP broadcasts. The range is from 1 to 999999.

Command Default

By default, the round-trip delay between the Cisco IOS software and an NTP broadcast server is 3000 microseconds.

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.
12.4(20)T	This command was modified. Support for NTPv4 and IPv6 was added.
12.2(33)SXJ	This command was modified. Support for NTPv4 and IPv6 was added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

Use the **ntp broadcastdelay** command when the router is configured as a broadcast client and the round-trip delay on the network is other than 3000 microseconds. In IPv6, the value set by this command should be used only when the **ntp broadcast client** and **ntp multicast client** commands have the **novolley** keyword enabled.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp broadcastdelay** command, the NTP service is activated (if it has not already been activated) and the estimated round-trip delay between the Cisco IOS software and an NTP broadcast server is set simultaneously.

In the **no** form of any **ntp** command, all the keywords are optional. When you enter the **no ntp broadcastdelay** command, only the estimated round-trip delay between the Cisco IOS software and an NTP broadcast server is removed from the NTP service. The NTP service itself remains active, along with any other functions you previously configured.

To disable the NTP service on a device, you must enter the **no ntp** command without any keywords in global configuration mode. For example, if you previously issued the **ntp broadcastdelay** command and you now want to remove not only the delay setting, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

Examples

The following example shows how to set the estimated round-trip delay between a router and the broadcast client to 5000 microseconds:

```
Router(config)# ntp broadcastdelay 5000
```

The following example shows how to remove all the configured NTP options and disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
ntp broadcast client	Configures the specified interface to receive NTP broadcast packets.
ntp multicast client	Configures the system to receive NTP multicast packets on a specified interface.

ntp disable

To prevent an interface from receiving Network Time Protocol (NTP) packets, use the **ntp disable** command in interface configuration mode. To enable the receipt of NTP packets on an interface, use the **no** form of this command.

ntp disable [**ip** | **ipv6**]

no ntp disable [**ip** | **ipv6**]

Syntax Description

ip	(Optional) Disables IP-based NTP traffic.
ipv6	(Optional) Disables IPv6-based NTP traffic.

Command Default

By default, interfaces receive NTP packets.

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.
12.4(20)T	This command was modified. Support for IPv6 was added. The optional **ip** and **ipv6** keywords were added.
12.2(33)SXJ	This command was modified. Support for IPv6 was added. The optional **ip** and **ipv6** keywords were added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

This command provides a simple method of access control.

Use the **ntp disable** command in interface configuration mode to configure an interface to reject NTP packets. If the **ntp disable** command is configured on an interface that does not have any NTP service running, the interface remains disabled even after the NTP service is started by another NTP configuration. When you use the **ntp disable** command without the **ip** or **ipv6** keyword, NTP is disabled on the interface for all the address families.

When you enter the **no ntp disable** command in interface configuration mode, the interface that was configured to reject NTP packets is enabled to receive NTP packets.

Note Remove all NTP commands from an interface before entering the **ntp disable** command on that interface.

Configuring the **ntp disable** command on an interface does not stop the NTP service. To disable the NTP service on a device, use the **no ntp** command without keywords in global configuration mode. For example, if you had previously issued the **ntp disable** command and you now want to remove not only this restriction, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

Examples

The following example shows how to prevent Ethernet interface 0 from receiving NTP packets:

```
Router(config)# interface ethernet 0
Router(config-if)# ntp disable
```

The following example shows the message displayed when you try to execute the **ntp disable** command on an interface that has other NTP commands configured on it:

```
Router(config-if)# ntp disable

%NTP: Unconfigure other NTP commands on this interface before executing 'ntp disable'
```

If you had previously issued the **ntp disable** command and you now want to remove not only this restriction, but also all NTP functions from the device, use the **no ntp** command without keywords in global configuration mode. The following example shows how to disable the NTP service on a device:

```
Router(config)# no ntp
```

Related Commands

Command	Description
ntp	Activates the NTP service.

ntp clear drift

To reset the drift value stored in the persistent data file, use the **ntp clear drift** command in privileged EXEC mode.

ntp clear drift

Syntax Description

This command has no arguments or keywords.

Command Default

The drift value stored in the persistent data file is not reset.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SXJ	This command was integrated into Cisco IOS Release 12.2(33)SXJ.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

The **ntp clear drift** command is used to reset the local clock drift value in the persistent data file. The drift is the frequency offset between the local clock hardware and the authoritative time from the Network Time Protocol version 4 (NTPv4) servers. NTPv4 automatically computes this drift and uses it to compensate permanently for local clock imperfections.

This command is available only when the NTP service is activated using any **ntp** command in global configuration mode.

Examples

The following example shows how to reset the drift value in the persistent data file:

```
Router# ntp clear drift
```

Related Commands

Command	Description
ntp	Activates the NTP service.

ntp logging

To enable Network Time Protocol (NTP) message logging, use the **ntp logging** command in global configuration mode. To disable NTP logging, use the **no** form of this command.

ntp logging

no ntp [**logging**]

Syntax Description

This command has no arguments or keywords.

Command Default

NTP message logging is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(7)T	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.
12.4(20)T	This command was modified. Support for IPv6 was added.
12.2(33)SXJ	This command was modified. Support for IPv6 was added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

Use the **ntp logging** command to control the display of NTP logging messages.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp logging** command, the NTP service is activated (if it has not already been activated) and message logging is enabled simultaneously.

In the **no** form of any **ntp** command, all the keywords are optional. When you enter the **no ntp logging** command, only message logging is disabled in the NTP service. The NTP service itself remains active, along with any other functions that you previously configured.

To disable the NTP service on a device, you must enter the **no ntp** command without keywords. For example, if you previously issued the **ntp logging** command and you now want to disable not only the message logging, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

Examples

The following example shows how to enable NTP message logging and verify that it is enabled:

```
Router# configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# ntp logging
Router(config)# end

Router# show running-config | include ntp
ntp logging
ntp clock-period 17180152
ntp peer 10.0.0.1
ntp server 192.168.166.3
```

The following example shows how to disable NTP message logging and verify to that it is disabled:

```
Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# no ntp logging
Router# end
Router(config)# show running-config | include ntp

ntp clock-period 17180152
ntp peer 10.0.0.1
ntp server 192.168.166.3
```

The following example shows how to remove all the configured NTP options and disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
ntp peer	Configures the software clock to synchronize a peer or to be synchronized by a peer.
ntp server	Allows the software clock to be synchronized by an NTP time server.

ntp master

To configure the Cisco IOS software as a Network Time Protocol (NTP) master clock to which peers synchronize themselves when an external NTP source is not available, use the **ntp master** command in global configuration mode. To disable the master clock function, use the **no** form of this command.

ntp master [*stratum*]

no ntp [**master**]

Caution Use this command with caution. Valid time sources can be easily overridden using this command, especially if a low stratum number is configured. Configuring multiple devices in the same network with the **ntp master** command can cause instability in keeping time if the devices do not agree on the time.

Syntax Description

stratum	(Optional) Number from 1 to 15. Indicates the NTP stratum number that the system will claim.

Command Default

By default, the master clock function is disabled. When enabled, the default stratum is 8.

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.
12.4(20)T	This command was modified. Support for IPv6 was added.
12.2(33)SXJ	This command was modified. Support for IPv6 was added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

Because the Cisco implementation of NTP does not support directly attached radio or atomic clocks, the router is normally synchronized, directly or indirectly, to an external system that has such a clock. In a network without Internet connectivity, such a time source may not be available. The **ntp master** command is used in such cases.

A system with the **ntp master** command configured that cannot reach any clock with a lower stratum number will claim to be synchronized at the configured stratum number, and other systems will be willing to synchronize to it via NTP.

Note The software clock must have been set from some source, including manual setting, before the **ntp master** command will have any effect. This protects against distributing erroneous time after the system is restarted.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp master** command, the NTP service is activated (if it has not already been activated) and the Cisco IOS software is configured as an NTP master clock simultaneously. When you enter the **no ntp master** command, only the NTP master clock configuration is removed from the NTP service. The NTP service itself remains active, along with any other functions that you previously configured.

To disable the NTP service on a device, you must enter the **no ntp** command without any keywords in global configuration mode. For example, if you had previously issued the **ntp master** command and you now want to remove not only the master clock function, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

Examples

The following example shows how to configure a router as an NTP master clock to which peers may synchronize:

```
Router(config)# ntp master 10
```

The following example shows how to remove all the configured NTP options and disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
clock calendar-valid	Configures the system hardware clock that is an authoritative time source for the network.

ntp max-associations

To configure the maximum number of Network Time Protocol (NTP) peers and clients for a routing device, use the **ntp max-associations** command in global configuration mode. To return the maximum associations value to the default, use the **no** form of this command.

ntp max-associations *number*

no ntp [**max-associations**]

Syntax Description

number	Number of NTP associations. The range is from 1 to 4294967295. The default is 100. In the Cisco IOS Release 12.2SX train, the range is from 0 to 4294967295.

Command Default

The maximum association value of NTP peers and clients is 100.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0	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.
12.4(20)T	This command was modified. Support for IPv6 was added.
12.2(33)SXJ	This command was modified. Support for IPv6 was added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

The router can be configured to define the maximum number of NTP peer and client associations that the router will serve. Use the **ntp max-associations** command to set the maximum number of NTP peer and client associations that the router will serve.

The **ntp max-associations** command is useful for ensuring that the router is not overwhelmed by NTP synchronization requests. For an NTP master server, this command is useful for allowing numerous devices to synchronize to a router.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp max-associations** command, the NTP service is activated (if it has not already been activated) and the maximum number of NTP peers and clients is configured simultaneously.

In the **no** form of any **ntp** command, all the keywords are optional. When you enter the **no ntp max-associations** command, only the maximum number value is removed from the NTP service. The NTP service itself remains active, along with any other functions that you previously configured.

To disable the NTP service on a device, you must enter the **no ntp** command without any keywords in global configuration mode. For example, if you previously issued the **ntp max-associations** command and you now want to remove not only that maximum value, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

Note By default, the previous configuration values are retained when the last valid configuration (configuration for which the NTP service needs to run) is removed. Only the configuration values related to the maximum number of NTP peer and client associations are reset to the default value when the NTP process is disabled.

Examples

In the following example, the router is configured to act as an NTP server to 200 clients:

```
Router(config)# ntp max-associations 200
```

The following example shows how to remove all the configured NTP options and disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
show ntp associations	Displays all current NTP associations for the device.

ntp multicast

To configure a system to send Network Time Protocol (NTP) multicast packets on a specified interface, use the **ntp multicast** command in interface configuration mode. To disable this capability, use the **no** form of this command.

ntp multicast [*ip-address* | *ipv6-address*] [**key** *key-id*] [**ttl** *value*] [**version** *number*]

no ntp [**multicast** [*ip-address* | *ipv6-address*] [**key** *key-id*] [**ttl** *value*] [**version** *number*]]

Syntax Description

ip-address	(Optional) IPv4 address of the multicast group. Default address is 224.0.1.1.
ipv6-address	(Optional) IPv6 address of the multicast group. The address can be the all-nodes IPv6 address (FF02::1) or any other IPv6 multicast address.
key	(Optional) Defines a multicast authentication key.
key-id	(Optional) Authentication key number in the range from 1 to 4294967295. In the Cisco IOS Release 12.2SX train, the range is from 0 to 4294967295.
ttl	(Optional) Defines the time-to-live (TTL) value of a multicast NTP packet.
value	(Optional) TTL value in the range from 1 to 255. Default TTL value is 16.
version	(Optional) Defines the NTP version number.
number	(Optional) NTP version number in the range from 2 to 4. Default version number for IPv4 is 3, and default number for IPv6 is 4. In the Cisco IOS Release 12.2SX train, the range is from 1 to 4.

Command Default

NTP multicast capability is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.1	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.
12.4(20)T	This command was modified. Support for NTPv4 and IPv6 was added. The *ipv6-address* argument was added.
12.2(33)SXJ	This command was modified. Support for NTPv4 and IPv6 was added. The *ipv6-address* argument was added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

The TTL value is used to limit the scope of an audience for multicast routing.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp multicast** command, the NTP service is activated (if it has not already been activated) and the interface on which to send multicast packets is configured simultaneously.

In the **no** form of any **ntp** command, all the keywords are optional. When you enter the **no ntp multicast** command, only the multicast capability is removed from the NTP service. The NTP service itself remains active, along with any other functions that you previously configured.

To disable the NTP service on a device, you must enter the **no ntp** command in global configuration mode without keywords. For example, if you had previously issued the **ntp multicast** command and you now want to remove not only the multicast capability, but also all NTP functions from the device, use the **no ntp** command in global configuration mode without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

Examples

The following example shows how to configure Ethernet interface 0 to send NTP version 2 broadcasts:

```
Router(config)# interface ethernet 0
Router(config-if)# ntp multicast version 2
```

If you had previously issued the **ntp multicast** command and you now want to remove not only the multicast capability, but also all NTP functions from the device, use the **no ntp** command in global configuration mode without any keywords. The following example shows how to remove the **ntp multicast** command along with all the other configured NTP options and to disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
ntp authentication-key	Defines an authentication key for NTP.
ntp multicast client	Allows the system to receive NTP multicast packets on an interface.

ntp multicast client

To configure the system to receive Network Time Protocol (NTP) multicast packets on a specified interface, use the **ntp multicast client** command in interface configuration mode. To disable this capability, use the **no** form of this command.

ntp multicast client [*ip-address* | *ipv6-address*] [**novolley**]

no ntp [**multicast client** [*ip-address* | *ipv6-address*]]

Syntax Description

ip-address	(Optional) IPv4 address of the multicast group. Default address is 224.0.1.1.
ipv6-address	(Optional) IPv6 address of the multicast group. The address can be the all-nodes IPv6 address (FF02::1) or any other IPv6 multicast address.
novolley	(Optional) Disables any messages sent to the broadcast server. Avoids propagation delay by using the value configured by the **ntp broadcastdelay** command.

Command Default

NTP multicast client capability is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.1	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.
12.4(20)T	This command was modified. Support for IPv6 was added. The *ipv6-address* argument and **novolley** keyword were added.
12.2(33)SXJ	This command was modified. Support for IPv6 was added. The *ipv6-address* argument and **novolley** keyword were added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

Use the **ntp multicast client** command to allow the system to listen to multicast packets on an interface-by-interface basis.

This command enables the multicast client mode on the local NTP host. In this mode, the host is ready to receive mode 5 (broadcast) NTP messages sent to the specified multicast address. After receiving the first packet, the client measures the nominal propagation delay using a brief client/server association with the server. After this initial phase, the client enters the broadcast client mode, in which it synchronizes its clock to the received multicast messages.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp multicast client** command, the NTP service is activated (if it has not already been activated) and the interface on which to receive multicast packets is configured simultaneously.

In the **no** form of any **ntp** command, all the keywords are optional. When you enter the **no ntp multicast client** command, only the multicast client capability is removed from the NTP service. The NTP service itself remains active, along with any other functions that you previously configured.

To disable the NTP service on a device, you must enter the **no ntp** command without any keywords in global configuration mode. For example, if you had previously issued the **ntp multicast client** command and you now want to remove not only the multicast client capability, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

In IPv6 configuration, the **ntp broadcastdelay** command is used when the **ntp broadcast client** or **ntp multicast client** command is configured with the **novolley** keyword.

Examples

In the following example, the system is configured to receive (listen to) NTP multicast packets on Ethernet interface 1:

```
Router(config)# interface ethernet 1
Router(config-if)# ntp multicast client
```

If you had previously issued the **ntp multicast client** command and you now want to remove not only the multicast client capability, but also all NTP functions from the device, use the **no ntp** command without any keywords. The following example shows how to remove the **ntp multicast client** command along with all the other configured NTP options and to disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
ntp broadcast client	Configures the specified interface to receive NTP broadcast packets.
ntp broadcastdelay	Sets the estimated round-trip delay between the Cisco IOS software and an NTP broadcast server.

ntp peer

To configure the software clock to synchronize an NTP peer or to be synchronized by an NTP peer, use the **ntp peer** command in global configuration mode. To disable this capability, use the **no** form of this command.

ntp peer [**vrf** *vrf-name*] {*ip-address* | *ipv6-address* | [**ip** | **ipv6**] *hostname*} [**normal-sync**] [**version** *number*] [**key** *key-id*] [**source** *interface-type interface-number*] [**prefer**] [**maxpoll** *number*] [**minpoll** *number*] [**burst**] [**iburst**]

no ntp [**vrf** *vrf-name*] {*ip-address* | *ipv6-address* | [**ip** | **ipv6**] *hostname*}

Syntax Description

vrf *vrf-name*	(Optional) Specifies that the peer should use a named VPN routing and forwarding (VRF) instance for routing to the destination instead of to the global routing table.
ip-address	IPv4 address of the peer providing or being provided the clock synchronization.
ipv6-address	IPv6 address of the peer providing or being provided the clock synchronization.
ip	(Optional) Forces Domain Name System (DNS) resolution to be performed in the IPv4 address space.
ipv6	(Optional) Forces DNS resolution to be performed in the IPv6 address space.
hostname	Hostname of the peer that is providing or being provided the clock synchronization.
normal-sync	(Optional) Disables the rapid synchronization at startup.
version	(Optional) Defines the Network Time Protocol (NTP) version number.
number	(Optional) NTP version number (2 to 4). In the Cisco IOS Release 12.2(33)SX train, the range is from 1 to 4.
key	(Optional) Defines the authentication key.
key-id	(Optional) Authentication key to use when sending packets to this peer.
source	(Optional) Specifies that the source address must be taken from the specified interface.
interface-type	(Optional) Name of the interface from which to pick the IPv4 or IPv6 source address. For more information, use the question mark (?) online help function.
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.
prefer	(Optional) Makes this peer the preferred peer that provides synchronization.
maxpoll *number*	(Optional) Configures the maximum timing intervals, in seconds, between client requests sent to the server. The *number* argument ranges from 4 to 17, with 10 as the default.
minpoll *number*	(Optional) Configures the minimum timing intervals, in seconds, between client requests sent to the server. The *number* argument ranges from 4 to 17, with 6 as the default.

burst	(Optional) Enables burst mode. Burst mode allows the exchange of eight NTP messages (instead of two) during each poll interval in order to reduce the effects of network jitter.
iburst	(Optional) Enables initial burst (iburst) mode. Iburst mode triggers the immediate exchange of eight NTP messages (instead of two) when an association is first initialized. This feature allows rapid time setting at system startup or when an association is configured.

Command Default

No peers are configured.
The default **maxpoll** *number* is 10 seconds.
The default **minpoll** *number* is 6 seconds.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.3(14)T	This command was modified. The **normal-sync** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was 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.
12.4(20)T	This command was modified. Support for IPv6 and NTPv4 was added. The **ip**, **ipv6**, **maxpoll**, **minpoll**, **burst**, and **iburst** keywords and the *ipv6-address* and *number* arguments were added.
12.2(33)SXJ	This command was modified. Support for IPv6 and NTPv4 was added. The **ip**, **ipv6**, **maxpoll**, **minpoll**, **burst**, and **iburst** keywords and the *ipv6-address* and *number* arguments were added. The command behavior was modified to display a message after selection of an unsupported NTP version.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

When a peer is configured, the default NTP version number is 3, no authentication key is used, and the source address is taken from the outgoing interface.

Use this command to allow a device to synchronize with a peer, or vice versa. Use the **prefer** keyword to reduce switching between peers.

If you are using the default version of 3 and NTP synchronization does not occur, try using NTP version 2 (NTPv2). For IPv6, use NTP version 4.

If you select an NTP version that is not supported, a message is displayed.

If you are using NTPv4, the NTP synchronization takes more time to complete (unlike NTPv3, which synchronizes in seconds or a maximum of 1 to 2 minutes). The acceptable time for synchronization in NTPv4 is 15 to 20 minutes. To achieve faster NTP synchronization, enable the burst or iburst mode by using the **burst** or **iburst** keyword. With the burst or iburst mode configured, NTP synchronization takes about 1 to 2 minutes.

The exact time span required for the NTP synchronization while using NTPv4 cannot be derived accurately. It depends on the network topology and complexity.

Multiple configurations are not allowed for the same peer or server. If a configuration exists for a peer and you use the **ntp peer** command to configure the same peer, the new configuration will replace the old one.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp peer** command, the NTP service is activated (if it has not already been activated) and the peer is configured simultaneously.

When you enter the **no ntp peer** command, only the NTP peer configuration is removed from the NTP service. The NTP service itself remains active, along with any other previously configured NTP functions.

To disable the NTP service on a device, use the **no ntp** command without keywords in global configuration mode. For example, if you had previously issued the **ntp peer** command and you now want to remove not only this restriction, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

Examples

The following example shows how to configure a router to allow its software clock to be synchronized with the clock of the peer (or vice versa) at the IPv4 address 192.168.22.33 using NTPv2. The source IPv4 address is the address of Ethernet 0:

```
Router(config)# ntp peer 192.168.22.33 version 2 source ethernet 0
```

The following example shows how to configure a router to allow its software clock to be synchronized with the clock of the peer (or vice versa) at IPv6 address 2001:0DB8:0:0:8:800:200C:417A using NTPv4:

```
Router(config)# ntp peer 2001:0DB8:0:0:8:800:200C:417A version 4
```

The following example shows how to disable rapid synchronization at startup:

```
Router(config)# ntp peer 192.168.22.33 normal-sync
```

The following example shows the message displayed when you try to configure an unsupported NTP version:

```
Router(config)# ntp peer 192.168.22.33 version 1

NTP version 4 supports backward compatibility to only version 2 and 3
 Please re-enter version[2-4]
 Setting NTP version 4 as default
```

The following example shows how to remove all the configured NTP options and disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
ntp authentication-key	Defines an authentication key for NTP.
ntp server	Allows the software clock to be synchronized by a time server.
ntp source	Uses a particular source address in NTP packets.

ntp refclock

To configure an external clock source for use with Network Time Protocol (NTP) services, use the **ntp refclock** command in line configuration mode. To disable support of the external time source, use the **no** form of this command.

ntp refclock {**trimble** | **telecom-solutions**} **pps** {**cts** | **ri** | **none**} [**inverted**] [**pps-offset** *milliseconds*] [**stratum** *number*] [**timestamp-offset** *number*]

no ntp [**refclock**]

Syntax Description

trimble	Enables the reference clock driver for the Trimble Palisade NTP Synchronization Kit (Cisco 7200 series routers only).
telecom-solutions	Enables the reference clock driver for a Telecom Solutions Global Positioning System (GPS) device.
pps	Enables a pulse per second (PPS) signal line. Indicates PPS pulse reference clock support. The options are **cts**, **ri**, or **none**.
cts	Enables PPS on the Clear To Send (CTS) line.
ri	Enables PPS on the Ring Indicator (RI) line.
none	Specifies that no PPS signal is available.
inverted	(Optional) Specifies that the PPS signal is inverted.
pps-offset *milliseconds*	(Optional) Specifies the offset of the PPS pulse. The number is the offset (in milliseconds).
stratum *number*	(Optional) Indicates the NTP stratum number that the system will claim. Number is from 0 to 14.
timestamp-offset *number*	(Optional) Specifies the offset of time stamp. The number is the offset (in milliseconds).

Command Default

By default, an external clock source for use with NTP services is not configured.

Command Modes

Line configuration (config-line)

Command History

Release	Modification
12.1	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.
12.4(20)T	This command was modified. Support for IPv6 was added.
12.2(33)SXJ	This command was modified. Support for IPv6 was added.

Release	Modification
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

To configure a PPS signal as the source for NTP synchronization, use the following form of the **ntp refclock** command:

ntp refclock trimble pps {**cts** | **ri**} [**inverted**] [**pps-offset** *milliseconds*] [**stratum** *number*] [**timestamp-offset** *number*]

To configure a Trimble Palisade NTP Synchronization Kit as the GPS clock source connected to the auxiliary port of a Cisco 7200 router, use the following form of the **ntp refclock** command:

ntp refclock trimble pps none [**stratum** *number*]

To configure a Telecom Solutions product as the GPS clock source, use the **ntp refclock telecom-solutions** form of the command:

ntp refclock telecom-solutions pps cts [**stratum** *number*]

When two or more servers are configured with the same stratum number, the client will never synchronize with any of the servers. This is because the client is not able to identify the device with which to synchronize. When two or more servers are configured with the same stratum number, and if the client was in synchronization with one of the servers, the synchronization is lost if the settings on one server are changed.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp refclock** command, the NTP service is activated (if it has not already been activated) and the external clock source is configured simultaneously.

In the **no** form of any **ntp** command, all the keywords are optional. When you enter the **no ntp refclock** command, only the external clock source is removed from the NTP service. The NTP service itself remains active, along with any other functions that you previously configured.

To terminate the NTP service on a device, you must enter the **no ntp** command without keywords in global configuration mode. For example, if you had previously issued the **ntp refclock** command and you now want to remove not only the external clock source, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also terminated.

Examples

The following example shows the configuration of a Trimble Palisade GPS time source on a Cisco 7200 router:

```
Router(config)# ntp master
Router(config)# ntp update-calendar
Router(config)# line aux 0
Router(config-line)# ntp refclock trimble pps none
```

The following example shows the configuration of a Telecom Solutions GPS time source on a Catalyst switch platform:

```
Router(config)# ntp master
Router(config)# ntp update-calendar
Router(config)# line aux 0
Router(config-line)# ntp refclock telecom-solutions pps cts stratum 1
```

If you had previously issued the **ntp refclock** command and you now want to remove not only the external clock source, but also all NTP functions from the device, use the **no ntp** command without any keywords in global configuration mode. The following example shows how to remove the **ntp refclock** command along with all the configured NTP options and how to disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
show ntp associations	Displays the status of NTP associations configured for your system.

ntp server

To allow the software clock to be synchronized by a Network Time Protocol (NTP) time server, use the **ntp server** command in global configuration mode. To disable this capability, use the **no** form of this command.

ntp server [**vrf** *vrf-name*] {*ip-address* | *ipv6-address* | [**ip** | **ipv6**] *hostname*} [**normal-sync**] [**version** *number*] [**key** *key-id*] [**source** *interface-type interface-number*] [**prefer**] [**maxpoll** *number*] [**minpoll** *number*] [**burst**] [**iburst**]

no ntp server [**vrf** *vrf-name*] {*ip-address* | *ipv6-address* | [**ip** | **ipv6**] *hostname*}

Syntax Description

vrf *vrf-name*	(Optional) Specifies that the peer should use a named VPN routing forwarding (VRF) instance for routing to the destination instead of to the global routing table.
ip-address	IPv4 address of the peer providing or being provided the clock synchronization.
ipv6-address	IPv6 address of the peer providing or being provided the clock synchronization.
ip	(Optional) Forces domain name server (DNS) resolution to be performed in the IPv4 address space.
ipv6	(Optional) Forces DNS resolution to be performed in the IPv6 address space.
hostname	Hostname of the peer providing or being provided the clock synchronization.
normal-sync	(Optional) Disables the rapid synchronization at startup.
version	(Optional) Defines the NTP version number.
number	(Optional) NTP version number (2 to 4). In the Cisco IOS Release 12.2SX train, the range is from 1 to 4.
key	(Optional) Defines the authentication key.
key-id	(Optional) Authentication key to use when sending packets to this peer.
source	(Optional) Specifies that the source address must be taken from the specified interface.
interface-type	(Optional) Name of the interface from which to pick the IPv4 or IPv6 source address. For more information, use the question mark (?) online help function.
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.
prefer	(Optional) Makes this peer the preferred peer that provides synchronization.
maxpoll *number*	(Optional) Configures the maximum timing intervals, in seconds, between client requests sent to the server. The *number* argument ranges from 4 to 17, with 10 as the default.
minpoll *number*	(Optional) Configures the minimum timing intervals, in seconds, between client requests sent to the server. The *number* argument ranges from 4 to 17, with 6 as the default.

burst	(Optional) Enables burst mode. Burst mode allows the exchange of eight NTP messages (instead of two) during each poll interval in order to reduce the effects of network jitter.
iburst	(Optional) Enables initial burst (iburst) mode. Iburst mode triggers the immediate exchange of eight NTP messages (instead of two) when an association is first initialized. This feature allows rapid time setting at system startup or when an association is configured.

Command Default

No servers are configured by default. If a server is configured, the default NTP version number is 3, an authentication key is not used, and the source IPv4 or IPv6 address is taken from the outgoing interface.

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 was integrated into the Cisco 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. Support for IPv6 was added to NTP version 4. The **ip**, **ipv6**, **maxpoll**, **minpoll**, **burst**, and **iburst** keywords and the *number* and *ipv6-address* arguments were added.
12.2(33)SXJ	This command was modified. Support for IPv6 was added to NTP version 4. The **ip**, **ipv6**, **maxpoll**, **minpoll**, **burst**, and **iburst** keywords and the *number* and *ipv6-address* arguments were added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

Use this command if you want to allow the system to synchronize with the specified server.

When you use the *hostname* option, the router does a DNS lookup on that name, and stores the IPv4 or IPv6 address in the configuration. For example, if you enter the **ntp server** *hostname* command and then check the running configuration, the output shows "ntp server *a.b.c.d*," where *a.b.c.d* is the IP address of the host, assuming that the router is correctly configured as a DNS client.

Use the **prefer** keyword if you need to use this command multiple times, and you want to set a preferred server. Using the **prefer** keyword reduces switching between servers.

If you are using the default NTP version 3 and NTP synchronization does not occur, try NTPv2. Some NTP servers on the Internet run version 2. For IPv6, use NTP version 4.

If you are using NTPv4, the NTP synchronization takes more time to complete (unlike NTPv3, which synchronizes in seconds or a maximum of 1 to 2 minutes). The acceptable time for synchronization in NTPv4 is 15 to 20 minutes. To achieve faster NTP synchronization, enable the burst or iburst mode by using the **burst** or **iburst** keyword. With the burst or iburst mode configured, NTP synchronization takes about 1 to 2 minutes.

The exact time span required for the NTP synchronization while using NTPv4 cannot be derived accurately. It depends on the network topology and complexity.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp server** command, the NTP service is activated (if it has not already been activated) and software clock synchronization is configured simultaneously.

When you enter the **no ntp server** command, only the server synchronization capability is removed from the NTP service. The NTP service itself remains active, along with any other previously configured NTP functions.

To disable the NTP service on a device, enter the **no ntp** command without keywords. For example, if you had previously issued the **ntp server** command and you now want to remove not only the server synchronization capability, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

If you want to unconfigure an NTP server or a peer configured with a particular source interface, you must specify the interface type and number in the **no** form of the command.

Examples

The following example shows how to configure a router to allow its software clock to be synchronized with the clock by using the device at the IPv4 address 172.16.22.44 using NTPv2:

```
Router(config)# ntp server 172.16.22.44 version 2
```

The following example shows how to configure a router to allow its software clock to be synchronized with the clock by using the device at the IPv6 address 2001:0DB8:0:0:8:800:200C:417A using NTPv4:

```
Router(config)# ntp server 2001:0DB8:0:0:8:800:200C:417A version 4
```

The following example shows how to configure an NTP peer with a particular source interface:

```
Router(config)# ntp server 209.165.200.231 source ethernet 0/1
```

Related Commands

Command	Description
ntp authentication-key	Defines an authentication key for NTP.
ntp peer	Configures the software clock to synchronize a peer or to be synchronized by a peer.
ntp source	Uses a particular source address in NTP packets.

ntp source

To use a particular source address in Network Time Protocol (NTP) packets, use the **ntp source** command in global configuration mode. To remove the specified source address, use the **no** form of this command.

ntp source *interface-type interface-number*

no ntp [**source**]

Syntax Description

interface-type	Type of interface.
interface-number	Number of the interface.

Command Default

Source address is determined by the outgoing interface.

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.
12.4(20)T	This command was modified. Support was added to allow a specified interface to be configured with IPv6 addresses.
12.2(33)SXJ	This command was modified. Support was added to allow a specified interface to be configured with IPv6 addresses.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

Use this command when you want to use a particular source IPv4 or IPv6 address for all NTP packets. The address is taken from the named interface. This command is useful if the address on an interface cannot be used as the destination for reply packets. If the **source** keyword is present on an **ntp server** or **ntp peer** global configuration command, that value overrides the global value set by this command.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp source** command, the NTP service is activated (if it has not already been activated) and the source address is configured simultaneously.

In the **no** form of any **ntp** command, all the keywords are optional. When you enter the **no ntp source** command, only the source address is removed from the NTP service. The NTP service itself remains active, along with any other functions that you previously configured.

To disable the NTP service on a device, you must enter the **no ntp** command without any keywords in global configuration mode. For example, if you had previously issued the **ntp source** command and you now want to remove not only the configured source address, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

If the NTP source is not set explicitly, and a link fails or an interface state changes, the NTP packets are sourced from the next best interface and the momentarily lost synchronization is regained.

Examples

The following example shows how to configure a router to use the IPv4 or IPv6 address of Ethernet interface 0 as the source address of all outgoing NTP packets:

```
Router(config)# ntp source ethernet 0
```

The following example shows how to remove all the configured NTP options and disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
ntp peer	Configures the software clock to synchronize a peer or to be synchronized by a peer.
ntp server	Allows the software clock to be synchronized by a time server.

ntp trusted-key

To authenticate the identity of a system to which Network Time Protocol (NTP) will synchronize, use the **ntp trusted-key** command in global configuration mode. To disable the authentication of the identity of the system, use the **no** form of this command.

ntp trusted-key *key-number*

no ntp [**trusted-key** *key-number*]

Syntax Description

key-number	Key number of the authentication key to be trusted.

Command Default

Authentication of the identity of the system is disabled.

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.
12.4(20)T	This command was modified. Support for IPv6 was added.
12.2(33)SXJ	This command was modified. Support for IPv6 was added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

If authentication is enabled, use this command to define one or more key numbers (corresponding to the keys defined with the **ntp authentication-key** command) that a peer NTP system must provide in its NTP packets for synchronization. This function provides protection against accidentally synchronizing the system to a system that is not trusted, because the other system must know the correct authentication key.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp trusted-key** command, the NTP service is activated (if it has not already been activated) and the system to which NTP will synchronize is authenticated simultaneously.

In the **no** form of any **ntp** command, all the keywords are optional. When you enter the **no ntp trusted-key** command, only the authentication is disabled in the NTP service. The NTP service itself remains active, along with any other functions that you previously configured.

To disable the NTP service on a device, you must enter the **no ntp** command without any keywords in global configuration mode. For example, if you had previously issued the **ntp trusted-key** command and you now want to remove not only the authentication, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

Examples

The following example shows how to configure the system to synchronize only to systems providing authentication key 42 in its NTP packets:

```
Router(config)# ntp authenticate
Router(config)# ntp authentication-key 42 md5 aNiceKey
Router(config)# ntp trusted-key 42
```

The following example shows how to remove all the configured NTP options and disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
ntp authenticate	Enables NTP authentication.
ntp authentication-key	Defines an authentication key for NTP.

ntp update-calendar

To periodically update the hardware clock (calendar) from a Network Time Protocol (NTP) time source, use the **ntp update-calendar** command in global configuration mode. To disable the periodic updates, use the **no** form of this command.

ntp update-calendar

no ntp [**update-calendar**]

Syntax Description

This command has no arguments or keywords.

Command Default

The hardware clock (calendar) is not updated.

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.
12.4(20)T	This command was modified. Support for IPv6 was added.
12.2(33)SXJ	This command was modified. Support for IPv6 was added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

Some platforms have a battery-powered hardware clock, referred to in the CLI as the calendar, in addition to the software-based system clock. The hardware clock runs continuously, even if the router is powered off or rebooted.

If the software clock is synchronized to an outside time source via NTP, it is a good practice to periodically update the hardware clock with the time learned from NTP. Otherwise, the hardware clock will tend to gradually lose or gain time (drift), and the software clock and hardware clock may lose synchronization with each other. The **ntp update-calendar** command will enable the hardware clock to be periodically updated with the time specified by the NTP source. The hardware clock will be updated only if NTP has synchronized to an authoritative time server.

Many lower-end routers (for example, the Cisco 2500 series or the Cisco 2600 series) do not have hardware clocks, so this command is not available on those platforms.

To force a single update of the hardware clock from the software clock, use the **clock update-calendar** command in user EXEC mode.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp update-calendar** command, the NTP service is activated (if it has not already been activated) and the hardware clock is updated simultaneously.

In the **no** form of any **ntp** command, all the keywords are optional. When you enter the **no ntp update-calendar** command, only the clock updates are stopped in the NTP service. The NTP service itself remains active, along with any other functions that you previously configured.

To disable the NTP service on a device, you must enter the **no ntp** command without any keywords in global configuration mode. For example, if you had previously issued the **ntp update-calendar** command and you now want to disable not only the periodic updates, but also all NTP functions running on the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

Examples

The following example shows how to configure the system to periodically update the hardware clock from the NTP time source:

```
Router(config)# ntp update-calendar
```

The following example shows how to remove all the configured NTP options and disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
clock read-calendar	Performs a one-time update of the software clock from the hardware clock (calendar).
clock update-calendar	Performs a one-time update of the hardware clock (calendar) from the software clock.

ospfv3 area

To enable Open Shortest Path First version 3 (OSPFv3) on an interface with the IPv4 or IPv6 address family (AF), use the **ospfv3 area** command in interface configuration mode. To disable OSPFv3 routing for interfaces defined, use the **no** form of this command.

ospfv3 *process-id* **area** *area-ID* {**ipv4** | **ipv6**} [**instance** *instance-id*]

no ospfv3 *process-id* **area** *area-ID* {**ipv4** | **ipv6**}

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
area-id	Area that is to be associated with the OSPFv3 interface.
ipv4	IPv4 address family.
ipv6	IPv6 address family.
instance *instance-id*	(Optional) Instance identifier. • When the **ipv4** keyword is used, the *instance-id* argument can be a value from 64 through 95. The default is 64. • When the **ipv6** keyword is used, the *instance-id* argument can be a value from 0 through 31. The default is 0.

Command Default

OSPFv3 is not enabled on the interface.
The default instance ID for IPv4 is 64.
The default instance ID for IPv6 is 0.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

Use the **ospfv3 area** command to enable OSPFv3 on an interface. This command enables you to configure two OSPFv3 instances on an interface–one IPv6 AF instance, and one IPv4 AF instance. You can configure only one process for each AF per interface.

Before you enable OSPFv3 on an interface using the **ospfv3 area** command, you must enable IPv6 on the interface, and you must enable IPv6 routing.

When the **ospfv3 area** command is configured for the IPv6 AF, it overwrites the **ipv6 ospf area** configuration if OSPFv3 was attached to the interface using the **ipv6 ospf area** command.

Examples

The following example enables OSPFv3 for the IPv4 AF on an interface:

```
Router(config)# interface ethernet0/0
Router(config-if)# ospfv3 1 area 1 ipv4
```

ospfv3 authentication

To specify the authentication type for an Open Shortest Path First version 3 (OSPFv3) instance, use the **ospfv3 authentication** command in interface configuration mode. To remove this instance, use the **no** form of this command.

ospfv3 authentication {**ipsec** *spi*} {**md5** | **sha1**} {*key-encryption-type key*} | **null**

no ospfv3 authentication {**ipsec** *spi*} {**md5** | **sha1**} {*key-encryption-type key*} | **null**

Syntax Description

ipsec	Configures use of IP Security (IPsec) authentication.
spi *spi*	Security policy index (SPI) value. The *spi* value must be a number from 256 to 4294967295.
md5	Enables message digest 5 (MD5) authentication.
sha1	Enables Secure Hash Algorithm 1 (SHA-1) authentication.
key-encryption-type	One of the following values can be entered: • **0**—The key is not encrypted. • **7**—The key is encrypted.
key	Number used in the calculation of the message digest. • When MD5 authentication is used, the key must be 32 hex digits (16 bytes) long. • When SHA-1 authentication is used, the key must be 40 hex digits (20 bytes) long.
null	Used to override area authentication.

Command Default

No authentication is specified.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

Use the **ospfv3 authentication** command to specify the OSPFv3 authentication type on an interface. The **ospfv3 authentication** command cannot be configured per process. If the **ospfv3 authentication** command is used, it affects all OSPFv3 instances.

The user needs to ensure that the same policy (the SPI and the key) is configured on all of the interfaces on the link. SPI values may automatically be used by other client applications, such as tunnels.

The policy database is common to all client applications on a box. This means that two IPsec clients, such as OSPFv3 and a tunnel, cannot use the same SPI. Additionally, an SPI can be used only in one policy.

The **null** keyword is used to override existing area authentication. If area authentication is not configured, then it is not necessary to configure the interface with the **authentication null** command.

Examples

The following example specifies the authentication type for an OSPFv3 instance: :

```
Router(config)# interface ethernet0/0
Router(config-if)# ospfv3 authentication md5 0 275761340947681324733020312097 27
```

Related Commands

Command	Description
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

ospfv3 cost

To explicitly specify the cost of sending a packet on an Open Shortest Path First version 3 (OSPFv3) interface, use the **ospfv3 cost** command in interface configuration mode. To reset the interface cost to the default value, use the **no** form of this command.

ospfv3 [*process-id*] **cost** {*interface-cost* | **dynamic** [**default** *default-link-metric* | **hysteresis** [*percent* | **threshold** *threshold-value*] | **weight** {**L2-factor** *percent* | **latency** *percent* | **resources** *percent* | **throughput** *percent*}

no ospfv3 [*process-id*] **cost**

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
interface-cost	Route cost of this interface. It can be a value in the range from 1 to 65535.
dynamic	Default value on VMI interfaces.
default	(Optional) Default link metric value.
default-link-metric	Specifies the default link metric value on this interface. It can be a value in the range from 0 to 65535.
hysteresis	(Optional) Hysteresis value for link-state advertisement (LSA) dampening.
percent	(Optional) The percentage of c
threshold *threshold-value*	(Optional) Cost change threshold at which hysteresis will be implemented. The threshold range is from 0 to 64k, and the default threshold value is 10k.
weight	(Optional) Amount of impact a variable has on the dynamic cost.
L2-factor *percent*	Quality weight of the Layer 2 link expressed as a percentage. The *percent* value can be in the range from 0 to 100. The default value is 100.
latency *percent*	Latency weight of the Layer 2 link, expressed as a percentage. The *percent* value can be in the range from 0 to 100. The default value is 100.
resources *percent*	Resources weight (such as battery life) of the router at the Layer 2 link, expressed as a percentage. The *percent* value can be in the range from 0 to 100. The default value is 100.
throughput *percent*	Throughput weight of the Layer 2 link, expressed as a percentage. The *percent* value can be in the range from 0 to 100. The default value is 100.

Command Default

Default cost is based on the bandwidth. Mobile Ad Hoc Network (MANET) interfaces are set to use dynamic costs. Non-MANET networks are set to use static costs.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

Use the **ospfv3 cost** command to specify the cost of sending a packet on an interface. When the **ospfv3 cost** command is configured with the *process-id* argument, it overwrites the **ipv6 ospf cost** configuration if OSPFv3 was attached to the interface using the **ipv6 ospf area** command. When the **ospfv3 cost** command is configured without the *process-id* argument, it is inherited on all instances running on the interface.

You can set the metric manually using the **ospfv3 cost** command, if you need to change the default. Using the **bandwidth** command changes the link cost as long as the **ospfv3 cost** command is not used. The link-state metric is advertised as the link cost in the router link advertisement.

The dynamic cost metric used for interfaces is computed based on the Layer 2 (L2) feedback to Layer 3 (L3). For a dynamic cost to have the same cost as a default cost, all parameters must equal zero.

Each Layer 2 feedback can contribute a cost in the range of 0 to 65535. To tune down this cost range, use the optional **weight** keyword in conjunction with the **throughput**, **resources**, **latency**, or **L2-factor** keyword. Each of these weights has a default value of 100% and can be configured in the range from 0 to 100. When 0 is configured for a specific weight, that weight does not contribute to the OSPFv3 cost.

Because cost components can change rapidly, you may need to dampen the amount of changes in order to reduce network-wide churn. Use the optional **hysteresis** keyword with the **threshold** *threshold-value* keyword and argument to set a cost change threshold. Any cost change below this threshold is ignored.

If you enable hysteresis without specifying the mode (percent or threshold), the default mode is threshold, and 10k as the default threshold value.

The higher the threshold or the percent value is set, the larger the change in link quality required to change the OSPFv3 route costs.

Mobile Ad Hoc Networks (MANET)

When the network type is set to MANET, the OSPF cost associated with an interface automatically sets to dynamic. All other network types, keep the interface cost, and you must enter the **ospfv3 cost dynamic** command to change the cost to dynamic.

If you do not specify a default dynamic cost with the **ospfv3 cost dynamic default** command, OSPF uses the interface cost until it receives link metric data.

Examples

The following example sets the interface cost value to 65:

```
Router(config)# interface ethernet0/0
Router(config-if)# ospfv3 101 cost 65
```

The following example shows how to configure OSPFv3 instance 4 to use 30 as the default cost until link metric data arrives from dynamic costing:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ospfv3 4 cost dynamic default 30
Router(config-if)# exit
```

Related Commands

Command	Description
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

ospfv3 database-filter

To filter outgoing link-state advertisements (LSAs) to an Open Shortest Path First version 3 (OSPFv3) interface, use the **database-filter** command in interface configuration mode. To restore the forwarding of LSAs to the interface, use the **no** form of this command.

ospfv3 [*process-id*] **database-filter** [**all** | **disable**]

no ospfv3 database-filter

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
all	(Optional) Filters all LSAs on the OSPFv3 interface.
disable	(Optional) Disables the LSA filter on the OSPFv3 interface.

Command Default

All outgoing LSAs are flooded to the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

Use the **ospfv3 database-filter** command to filter outgoing LSAs to an OSPFv3 interface. When the **ospfv3 database-filter** command is configured with the *process-id* argument, it overwrites the **ipv6 ospf database-filter** configuration if OSPFv3 was attached to the interface using the **ipv6 ospf area** command. When the **ospfv3 database-filter** command is configured without the *process-id* argument, it is inherited on all instances running on the interface.

Examples

The following example prevents flooding of OSPFv3 LSAs to networks reachable through Ethernet interface 0/0:

```
Router(config)# interface ethernet0/0
Router(config-if)# ospfv3 101 database-filter
```

Related Commands

Command	Description
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

ospfv3 dead-interval

To set the time period for which hello packets must not be seen before neighbors declare the router down, use the **ospfv3 dead-interval** command in interface configuration mode. To return to the default time, use the **no** form of this command.

ospfv3 [*process-id*] **dead-interval** *seconds*

no ospfv3 [*process-id*] **dead-interval** *seconds*

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
seconds	Specifies the interval (in seconds). The value must be the same for all nodes on the network. The value can be from 1 through 65335 seconds.

Command Default

Four times the interval set by the **ospfv3 hello-interval** command.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

Use the **ospfv3 dead-interval** command to set the time period for which hello packets must not be seen before neighbors declare the router down. When the **ospfv3 dead-interval** command is configured with the *process-id* argument, it overwrites the **ipv6 dead-interval** configuration if OSPFv3 was attached to the interface using the **ipv6 ospf area** command. When the **ospfv3 dead-interval** command is configured without the *process-id* argument, it is inherited on all instances running on the interface.

The interval is advertised in router hello packets. This value must be the same for all routers and access servers on a specific network.

If no hello-interval is specified, the default dead-interval is 120 seconds for Mobile Ad Hoc Networks (MANETs) and 40 seconds for all other network types.

Examples

The following example sets the OSPFv3 dead interval to 60 seconds:

```
Router(config)# interface ethernet0/0
Router(config-if)# ospfv3 101 dead-interval 60
```

Related Commands

Command	Description
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

ospfv3 demand-circuit

To configure Open Shortest Path First version 3 (OSPFv3) to treat the interface as an OSPFv3 demand circuit, use the **ospfv3 demand-circuit** command in interface configuration mode. To remove the demand circuit designation from the interface, use the **no** form of this command.

ospfv3 [*process-id*] **demand-circuit** [**disable**]

no ospfv3 demand-circuit

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
disable	(Optional) Disables the demand circuit on the specified OSPFv3 instance.

Command Default

The circuit is not a demand circuit.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

Use the **ospfv3 demand-circuit** command to configure OSPFv3 to treat the interface as an OSPFv3 demand circuit. When the **ospfv3 demand-circuit** command is configured with the *process-id* argument, it overwrites the **ipv6 ospf demand-circuit** configuration if OSPFv3 was attached to the interface using the **ipv6 ospf area** command. When the **ospfv3 demand-circuit** command is configured without the *process-id* argument, it is inherited on all instances running on the interface.

On point-to-point interfaces, only one end of the demand circuit must be configured with the **demand-circuit** command. Periodic hello messages are suppressed and periodic refreshes of link-state advertisements (LSAs) do not flood the demand circuit. This command allows the underlying data link layer to be closed when the topology is stable. In point-to-multipoint topology, only the multipoint end must configured with this command.

Examples

The following example configures an on-demand circuit on Ethernet interface 0/0:

```
Router(config)# interface ethernet0/0
Router(config-if)# ospfv3 101 demand-circuit
```

Related Commands

Command	Description
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

ospfv3 encryption

To specify the encryption type for an Open Shortest Path First version 3 (OSPFv3) interface, use the **ospfv3 encryption** command in interface configuration mode. To remove the encryption type from an interface, use the **no** form of this command.

ospfv3 encryption {**ipsec spi** *spi* **esp** *encryption-algorithm* {*key-encryption-type key*} *authentication-algorithm* {*key-encryption-type key*} | **null**}

no ospfv3 encryption ipsec spi *spi*

Syntax Description

ipsec	Configures use of IP Security (IPsec) authentication.
spi *spi*	Security policy index (SPI) value. The *spi* value must be a number from 256 to 4294967295.
esp	Encapsulating security payload (ESP).
encryption-algorithm	Encryption algorithm to be used with ESP. The values can be any of the following: • **aes-cdc**—Enables AES-CDC encryption. • **3des**—Enables 3DES encryption. • **des**—Enables DES encryption. • **null**—ESP with no encryption.
key-encryption-type	One of two values can be entered: • **0**—The key is not encrypted. • **7**—The key is encrypted.
key	Number used in the calculation of the message digest. • When MD5 authentication is used, the key must be 32 hex digits (16 bytes) long. • When SHA-1 authentication is used, the key must be 40 hex digits (20 bytes) long.
authentication-algorithm	Encryption authentication algorithm to be used. The values can be one of the following: • **md5**—Enables message digest 5 (MD5). • **sha1**—Enables SHA-1.
null	Overrides area encryption.

Command Default

Authentication and encryption are not configured on an interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

Use the **ospfv3 encryption** command to specify the encryption type for an interface. The **ospfv3 encryption** command cannot be configured per process. If the **ospfv3 encryption** command is used, it affects all OSPFv3 instances.

The user needs to ensure that the same policy (the SPI and the key) is configured on all of the interfaces on the link. SPI values may automatically be used by other client applications, such as tunnels.

The policy database is common to all client applications on a box. This means that two IPSec clients, such as OSPFv3 and a tunnel, cannot use the same SPI. Additionally, an SPI can be used only in one policy.

The **null** keyword is used to override existing area encryption. If area encryption is not configured, then it is not necessary to configure the interface with the **encryption null** command.

Examples

The following example specifies the encryption type for Ethernet interface 0/0. The IPSec SPI value is 1001, ESP is used with no encryption, and the authentication algorithm is MD5.

```
Router(config)# interface ethernet 0/0
Router(config-if)# ospfv3 encryption ipsec spi 1001 esp null md5 0
275761340947681324733020312097 27
```

Related Commands

Command	Description
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

ospfv3 flood-reduction

To suppress the unnecessary flooding of link-state advertisements (LSAs) in stable topologies, use the **ospfv3 flood-reduction** command in interface configuration mode. To disable this feature, use the **no** form of this command.

ospfv3 [*process-id*] **flood-reduction** [**disable**]

no ospfv3 [*process-id*] **flood-reduction**

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the Open Shortest Path First version 3 (OSPFv3) routing process and can be a value from 1 through 65535.
disable	(Optional) Allows flood reduction to be disabled on the specified OSPFv3 interface.

Command Default

This command is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

Use the **ospfv3 flood-reduction** command to suppress unnecessary LSA flooding in stable topologies. When the **ospfv3 flood-reduction** command is configured with the *process-id* argument, it overwrites the **ipv6 ospf flood-reduction** configuration if OSPFv3 was attached to the interface using the **ipv6 ospf flood-reduction** command. When the **ospfv3 flood-reduction** command is configured without the *process-id* argument, it is inherited on all instances running on the interface.

All routers supporting the OSPFv3 demand circuit are compatible and can interact with routers supporting flooding reduction.

Examples

The following example suppresses the flooding of unnecessary LSAs on Ethernet interface 0/0:

```
Router(config)# interface ethernet0/0
Router(config-if)# ospfv3 101 flood-reduction
```

Related Commands

Command	Description
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

ospfv3 hello-interval

To specify the interval between hello packets that the Cisco IOS software sends on the Open Shortest Path First version 3 (OSPFv3) interface, use the **ospfv3 hello-interval** command in interface configuration mode. To return to the default time, use the **no** form of this command.

ospfv3 [*process-id*] **hello-interval** *seconds*

no ospfv3 [*process-id*] **hello-interval** *seconds*

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
seconds	Specifies the interval (in seconds). The value must be the same for all nodes on a specific network.

Command Default

The default interval is 10 seconds when using Ethernet and 30 seconds when using nonbroadcast, such as Mobile Ad Hoc Networks (MANETs).

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

Use the **ospfv3 hello-interval** command to suppress unnecessary LSA flooding in stable topologies. When the **ospfv3 hello-interval** command is configured with the *process-id* argument, it overwrites the **ipv6 ospf hello-interval** configuration if OSPFv3 was attached to the interface using the **ipv6 ospf area** command. When the **ospfv3 hello-interval** command is configured without the *process-id* argument, it is inherited on all instances running on the interface.

The **hello-interval** value is advertised in the hello packets. The shorter the hello interval, the earlier topological changes will be detected, but more routing traffic will ensue. This value must be the same for all routers and access servers on a specific network.

Examples

The following example sets the interval between hello packets to 15 seconds:

```
Router(config)# interface ethernet0/0
Router(config-if)# ospfv3 101 hello-interval 15
```

Related Commands

Command	Description
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

ospfv3 mtu-ignore

To disable Open Shortest Path First version 3 (OSPFv3) maximum transmission unit (MTU) mismatch detection on receiving database descriptor (DBD) packets, use the **ospfv3 mtu-ignore** command in interface configuration mode. To reset to default, use the **no** form of this command.

ospfv3 [*process-id*] **mtu-ignore** [**disable**]

no ospfv3 [*process-id*] **mtu-ignore**

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
disable	(Optional) Allows **mtu-ignore** to be disabled on the specified OSPFv3 interface.

Command Default

OSPFv3 MTU mismatch detection is enabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

Use the **ospfv3 mtu-ignore** command to disable OSPFv3 MTU mismatch detection on receiving DBD packets. When the **ospfv3 mtu-ignore** command is configured with the *process-id* argument, it overwrites the **ipv6 ospf mtu-ignore** configuration if OSPFv3 was attached to the interface using the **ipv6 ospf area** command. When the **ospfv3 mtu-ignore** command is configured without the *process-id* argument, it is inherited on all instances running on the interface.

OSPFv3 checks whether neighbors are using the same MTU on a common interface. This check is performed when neighbors exchange DBD packets. If the receiving MTU in the DBD packet is higher then the IP MTU configured on the incoming interface, OSPFv3 adjacency will not be established.

Examples

The following example disables MTU mismatch detection on receiving DBD packets:

```
Router(config)# interface ethernet0/0
Router(config-if)# ospfv3 101 mtu-ignore
```

Related Commands

Command	Description
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

ospfv3 network

To configure an Open Shortest Path First version 3 (OSPFv3) network type to a type other than the default for a given medium, use the **ospfv3 network** command in interface configuration mode. To return to the default type, use the **no** form of this command.

ospfv3 [*process-id*] **network** {**broadcast** | **manet** | **non-broadcast** | {**point-to-multipoint** [**non-broadcast**] | **point-to-point**}}

no ospfv3 [*process-id*] **network** {**broadcast** | **manet** | **non-broadcast** | {**point-to-multipoint** [**non-broadcast**] | **point-to-point**}}

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
broadcast	Sets the network type to broadcast.
manet	Sets the network type to Mobile Ad Hoc Network (MANET).
non-broadcast	Sets the network type to nonbroadcast multiaccess (NBMA).
point-to-multipoint [**non-broadcast**]	Sets the network type to point-to-multipoint. The optional **non-broadcast** keyword sets the point-to-multipoint network to be nonbroadcast. If you use the **non-broadcast** keyword, the **neighbor** command is required.
point-to-point	Sets the network type to point-to-point.

Command Default

Default depends on the network type.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

Use the **ospfv3 network** command to configure an OSPFv3 network type to a type other than the default for a given medium. When the **ospfv3 network** command is configured with the *process-id* argument, it overwrites the **ipv6 ospf network** configuration if OSPFv3 was attached to the interface using the **ipv6 ospf area** command. When the **ospfv3 network** command is configured without the *process-id* argument, it is inherited on all instances running on the interface. .

MANET Networks

Use the **ospfv3 network manet** command to enable relaying and caching of LSA updates and LSA ACKs on the MANET interface. This results in a reduction of OSPF traffic and saves radio bandwidth.

By default, selective peering is disabled on MANET interfaces.

By default, the OSPFv3 dynamic cost timer is enabled for the MANET network type, as well as caching of LSAs and LSA ACKs received on the MANET interface. The following default values are applied for cache and timers:

LSA cache	Default = 1000 messages
LSA timer	Default = 10 minutes
LSA ACK cache	Default = 1000 messages
LSA ACK timer	Default = 5 minutes

Examples

The following example sets your OSPFv3 network as a broadcast network:

```
Router(config)# interface ethernet0/0
Router(config-if)# ospfv3 101 network broadcast
```

Related Commands

Command	Description
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

ospfv3 priority

To set the router priority, which helps determine the designated router for this network, use the **ospfv3 priority** command in interface configuration mode. To return to the default value, use the **no** form of this command.

ospfv3 [*process-id*] **priority** *number-value*

no ospfv3 [*process-id*] **priority** *number-value*

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the Open Shortest Path First version 3 (OSPFv3) routing process and can be a value from 1 through 65535.
number-value	A number value that specifies the priority of the router. The range is from 0 to 255.

Command Default

The router priority is 1.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

Use the **ospfv3 priority** command to set the router priority, which helps determine the designated router for this network. When the **ospfv3 priority** command is configured with the *process-id* argument, it overwrites the **ipv6 ospf priority** configuration if OSPFv3 was attached to the interface using the **ipv6 ospf area** command. When the **ospfv3 priority** command is configured without the *process-id* argument, it is inherited on all instances running on the interface.

When two routers attached to a network both attempt to become the designated router, the one with the higher router priority takes precedence. If there is a tie, the router with the higher router ID takes precedence. A router with a router priority set to zero is ineligible to become the designated router or backup designated router. Router priority is configured only for interfaces to multiaccess networks (in other words, not to point-to-point networks).

Examples

The following example sets the router priority value to 4:

```
Router(config)# interface ethernet0/0
Router(config-if)# ospfv3 101 priority 4
```

Related Commands

Command	Description
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

ospfv3 retransmit-interval

To specify the time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the Open Shortest Path First version 3 (OSPFv3) interface, use the **ospfv3 retransmit-interval** command in interface configuration mode. To return to the default value, use the **no** form of this command.

ospfv3 [*process-id*] **retransmit-interval** *seconds*

no ospfv3 [*process-id*] **retransmit-interval** *seconds*

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
seconds	Time (in seconds) between retransmissions. It must be greater than the expected round-trip delay between any two routers on the attached network. The range is from 1 to 65535 seconds, and the default is 5 seconds.

Command Default

The default is 5 seconds.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

Use the **ospfv3 retransmit-interval** command to specify the time between LSA retransmissions for adjacencies belonging to the interface. When the **ospfv3 retransmit-interval** command is configured with the *process-id* argument, it overwrites the **ipv6 ospf retransmit-interval** configuration if OSPFv3 was attached to the interface using the **ipv6 ospf area** command. When the **ospfv3 retransmit-interval** command is configured without the *process-id* argument, it is inherited on all instances running on the interface.

When a router sends an LSA to its neighbor, it keeps the LSA until it receives back the acknowledgment message. If the router receives no acknowledgment, it will resend the LSA.

The setting of the restransmit-interval parameter should be conservative, or needless retransmission will result. The value should be larger for serial lines and virtual links.

Examples

The following example sets the retransmit interval value to 8 seconds:

```
Router(config)# interface ethernet0/0
Router(config-if)# ospfv3 101 retransmit-interval 8
```

Related Commands

Command	Description
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

ospfv3 transmit-delay

To set the estimated time required to send a link-state update packet on the Open Shortest Path First version 3 (OSPFv3) interface, use the **ospfv3 transmit-delay** command in interface configuration mode. To return to the default value, use the **no** form of this command.

ospfv3 [*process-id*] **transmit-delay** *seconds*

no ospfv3 [*process-id*] **transmit-delay** *seconds*

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the Open Shortest Path First version 3 (OSPFv3) routing process and can be a value from 1 through 65535.
seconds	Time (in seconds) required to send a link-state update. The range is from 1 to 65535 seconds. The default is 1 second.

Command Default

The default is 1 second.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

Use the **ospfv3 transmit-delay** command to set the estimated time required to send a link-state update packet on the interface. When the **ospfv3 transmit-delay** command is configured with the *process-id* argument, it overwrites the **ipv6 ospf transmit-delay** configuration if OSPFv3 was attached to the interface using the **ipv6 ospf area** command. When the **ospfv3 transmit-delay** command is configured without the *process-id* argument, it is inherited on all instances running on the interface.

Link-state advertisements (LSAs) in the update packet must have their ages incremented by the amount specified in the *seconds* argument before transmission. The value assigned should take into account the transmission and propagation delays for the interface.

If the delay is not added before transmission over a link, the time in which the LSA propagates over the link is not considered. This setting has more significance on very low-speed links.

Examples

The following example sets the retransmit delay value to 3 seconds:

```
Router(config)# interface ethernet0/0
Router(config-if)# ospfv3 101 transmit-delay 3
```

Related Commands

Command	Description
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

other-config-flag

To verify the advertised other configuration parameter, use the **other-config-flag** command in router advertisement (RA) guard policy configuration mode.

other-config-flag {**on** | **off**}

Syntax Description

on	Verification is enabled.
off	Verification is disabled.

Command Default

Verification is not enabled.

Command Modes

RA guard policy configuration (config-ra-guard)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

The **other-config-flag** command enables verification of the advertised "other" configuration parameter (or "O" flag). This flag could be set by an attacker to force hosts to retrieve other configuration information through a potentially untrusted DHCPv6 server.

Examples

The following example defines an RA guard policy name as raguard1, places the router in RA guard policy configuration mode, and enables O flag verification:

```
Router(config)# ipv6 nd raguard policy raguard1
Router(config-ra-guard)# other-config-flag on
```

Related Commands

Command	Description
ipv6 nd raguard policy	Defines the RA guard policy name and enter RA guard policy configuration mode.

outbound-proxy

To configure a Session Initiation Protocol (SIP) outbound proxy for outgoing SIP messages globally on a Cisco IOS voice gateway, use the **outbound-proxy** command in voice service SIP configuration mode. To globally disable forwarding of SIP messages to a SIP outbound proxy globally, use the **no** form of this command.

outbound-proxy {**dhcp** | **ipv4:***ip-address*[**:***port-number*] | **dns:***host***:***domain* [**reuse**]}

no outbound-proxy

Syntax Description

dhcp	Specifies the SIP outbound proxy globally for a Cisco IOS voice gateway; all SIP dialog-initiating requests are sent to the SIP server obtained via DHCP.
ipv4:*ip-address*	Specifies the SIP outbound proxy globally for a Cisco IOS voice gateway; all SIP dialog-initiating requests are sent to this IP address. The colon is required.
:*port-number*	(Optional) The port to which all SIP dialog-initiating requests are sent at the specified IP address. Port number ranges from 0 to 65535. The default is 5060. The colon is required.
dns:*host***:***domain*	Specifies the SIP outbound proxy globally for a Cisco IOS voice gateway; all initiating requests are sent to the specified destination domain. The colon is required.
reuse	(Optional) Reuses the outbound proxy address established during registration for all subsequent registration refreshes and calls.

Command Default

The Cisco IOS voice gateway does not forward outbound SIP messages to a proxy.

Command Modes

Voice service VoIP SIP configuration (conf-serv-sip)

Command History

Release	Modification
12.4(15)T	This command was introduced.
12.4(22)T	Support for IPv6 was added.
12.4(22)YB	This command was modifed. The **dhcp** keyword was added.
15.0(1)M	This command was integrated in Cisco IOS Release 15.0(1)M.
15.1(2)T	This command was modified. The **reuse** keyword was added.

Usage Guidelines

You can use the **outbound-proxy** command in voice service SIP configuration mode to specify outbound proxy settings globally for a Cisco IOS voice gateway. You can also use the **voice-class sip outbound-proxy** command in dial peer voice configuration mode to configure settings for an individual dial peer that override or defer to the global settings for the gateway. However, if both a Cisco Unified Communications Manager Express (CME) and a SIP gateway are configured on the same router, then there is a scenario that can cause incoming SIP messages from line-side phones to be confused with SIP

messages coming from the network side. To avoid failed calls caused by this scenario, disable the SIP outbound proxy setting for all line-side phones on a dial peer using the **outbound-proxy system** command in voice register global configuration mode.

Examples

The following example shows how to specify the SIP outbound proxy globally for a Cisco IOS voice gateway using an IP address:

```
Router> enable
Router# configure terminal
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# outbound-proxy ipv4:10.1.1.1
```

The following example shows how to specify the SIP outbound proxy globally for a Cisco IOS voice gateway using a destination hostname and domain:

```
Router> enable
Router# configure terminal
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# outbound-proxy dns:sipproxy:example.com
```

The following example shows how to specify the SIP outbound proxy globally for a Cisco IOS voice gateway using the DHCP protocol:

```
Router> enable
Router# configure terminal
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# outbound-proxy dhcp
```

Related Commands

Command	Description
outbound-proxy system	Specifies whether Cisco Unified CME line-side SIP phones use the outbound proxy settings configured globally for a Cisco IOS voice gateway.
voice-class sip outbound-proxy	Configures SIP outbound proxy settings for an individual dial peer that override global settings for the Cisco IOS voice gateway.

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.
15.1(2)T	Support for IPv6 was 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.

Command	Description
inspect	Enables Cisco IOS stateful packet inspection.
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.
ipv6 routing-enforcement-header loose	Provides backward compatibility with legacy IPv6 inspection.
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.

passive-interface (IPv6)

To disable sending routing updates on an interface, use the **passive-interface** command in router configuration mode. To reenable the sending of routing updates, use the **no** form of this command.

passive-interface [**default** | *interface-type interface-number*]

no passive-interface [**default** | *interface-type interface-number*]

Syntax Description

default	(Optional) All interfaces become passive.
interface-type interface-number	(Optional) Interface type and number. For more information, use the question mark (**?**) online help function.

Command Default

No interfaces are passive. Routing updates are sent to all interfaces on which the routing protocol is enabled.

Command Modes

Router configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.4(6)T	Support for Enhanced Internal Gateway Routing Protocol (EIGRP) IPv6 was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
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.

Usage Guidelines

If you disable the sending of routing updates on an interface, the particular address prefix will continue to be advertised to other interfaces, and updates from other routers on that interface continue to be received and processed.

The **default** keyword sets all interfaces as passive by default. You can then configure individual interfaces where adjacencies are desired using the **no passive-interface** command. The **default** keyword is useful in Internet service provider (ISP) and large enterprise networks where many of the distribution routers have more than 200 interfaces.

OSPF for IPv6 routing information is neither sent nor received through the specified router interface. The specified interface address appears as a stub network in the OSPF for IPv6 domain.

For the Intermediate System-to-Intermediate System (IS-IS) protocol, this command instructs IS-IS to advertise the IP addresses for the specified interface without actually running IS-IS on that interface. The **no** form of this command for IS-IS disables advertising IP addresses for the specified address.

Examples

The following example sets all interfaces as passive, then activates Ethernet interface 0:

```
Router(config-router)# passive-interface default
Router(config-router)# no passive-interface ethernet0/0
```

passive-interface (OSPFv3)

To suppress sending routing updates on an interface when using an IPv4 Open Shortest Path First version 3 (OSPFv3) process, use the **passive-interface** command in router configuration mode. To reenable the sending of routing updates, use the **no** form of this command.

passive-interface [**default** | *interface-type interface-number*]

no passive-interface [**default** | *interface-type interface-number*]

Syntax Description

default	(Optional) All interfaces become passive.
interface-type interface-number	(Optional) Interface type and number. For more information, use the question mark (**?**) online help function.

Command Default

No interfaces are passive. Routing updates are sent to all interfaces on which the routing protocol is enabled.

Command Modes

OSPFv3 router configuration mode (config-router)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

If you suppress the sending of routing updates on an interface, the particular address prefix will continue to be advertised to other interfaces, and updates from other routers on that interface continue to be received and processed.

The **default** keyword sets all interfaces as passive by default. You can then configure individual interfaces where adjacencies are desired using the **no passive-interface** command. The **default** keyword is useful in Internet service provider (ISP) and large enterprise networks where many of the distribution routers have more than 200 interfaces.

Examples

The following example sets all interfaces as passive, then activates Ethernet interface 0/0:

```
Router(config-router)# passive-interface default
Router(config-router)# no passive-interface ethernet0/0
```

Related Commands

Command	Description
default (OSPFv3)	Returns an OSPFv3 parameter to its default value.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

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.

peer default ipv6 address pool

To specify the pool from which client prefixes are assigned, use the **peer default ipv6 address pool** command in interface configuration mode. To disable a prior peer IPv6 address pooling configuration on an interface, or to remove the default address from your configuration, use the **no** form of this command.

peer default ipv6 address pool *pool-name*

no peer default ipv6 address pool

Syntax Description

pool-name	Name of a local address pool created using the **ipv6 local pool** command.

Command Default

The default pool name is **pool**.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

This command applies to point-to-point interfaces that support PPP encapsulation. This command sets the address used on the remote (PC) side.

This command allows an administrator to configure all possible address pooling mechanisms on an interface-by-interface basis.

Examples

The following command specifies that this interface will use a local IPv6 address pool named pool3:

```
peer default ipv6 address pool pool3
```

In the following example, the pool1 pool is assigned to virtual template 1:

```
interface Virtual-Template1
 ipv6 enable
 no ipv6 nd suppress-ra
 peer default ipv6 address pool pool1
 ppp authentication chap
```

Related Commands

Command	Description
async dynamic address	Specifies dynamic asynchronous addressing versus default addressing.
encapsulation ppp	Enables PPP encapsulation.
exec	Allows an EXEC process on a line.
ipv6 local pool	Configures a local pool of IPv6 addresses to be used when a remote peer connects to a point-to-point interface.
ppp	Starts an asynchronous connection using PPP.

permit (IPv6)

To set permit conditions for an IPv6 access list, use the **permit** command in IPv6 access list configuration mode. To remove the permit conditions, use the **no** form of this command.

permit *protocol* {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**reflect** *name* [**timeout** *value*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]

no permit {*protocol*} {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**reflect** *name* [**timeout** *value*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]

Internet Control Message Protocol

permit icmp {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [*icmp-type* [*icmp-code*] | *icmp-message*] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]

Transmission Control Protocol

permit tcp {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [**ack**] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**established**] [**fin**] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**neq** {*port* | *protocol*}] [**psh**] [**range** {*port* | *protocol*}] [**reflect** *name* [**timeout** *value*]] [**routing**] [**routing-type** *routing-number*] [**rst**] [**sequence** *value*] [**syn**] [**time-range** *name*] [**urg**]

User Datagram Protocol

permit udp {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**neq** {*port* | *protocol*}] [**range** {*port* | *protocol*}] [**reflect** *name* [**timeout** *value*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]

Syntax Description

protocol	Name or number of an Internet protocol. It can be one of the keywords **ahp**, **esp**, **icmp**, **ipv6**, **pcp**, **sctp**, **tcp**, or **udp**, or an integer in the range from 0 to 255 representing an IPv6 protocol number.
source-ipv6-prefix/*prefix-length*	The source IPv6 network or class of networks about which to set permit conditions. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
any	An abbreviation for the IPv6 prefix ::/0.
host *source-ipv6-address*	The source IPv6 host address about which to set permit conditions. This *source-ipv6-address* argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
auth	Allows matching traffic against the presence of the authentication header in combination with the specified protocol; that is, TCP or UDP.
operator [*port-number*]	(Optional) Specifies an operand that compares the source or destination ports of the specified protocol. Operands are **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range** (inclusive range). If the operator is positioned after the *source-ipv6-prefix*/*prefix-length* argument, it must match the source port. If the operator is positioned after the *destination-ipv6-prefix*/*prefix-length* argument, it must match the destination port. The **range** operator requires two port numbers. All other operators require one port number. The optional *port-number* argument is a decimal number or the name of a TCP or UDP port. A port number is a number from 0 to 65535. TCP port names can be used only when filtering TCP. UDP port names can be used only when filtering UDP.
destination-ipv6-prefix/*prefix-length*	The destination IPv6 network or class of networks about which to set permit conditions. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
host *destination-ipv6-address*	The destination IPv6 host address about which to set permit conditions. This *destination-ipv6-address* argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
dest-option-type	(Optional) Matches IPv6 packets against the destination extension header within each IPv6 packet header.
doh-number	(Optional) Integer in the range from 0 to 255 representing an IPv6 destination option extension header.
doh-type	(Optional) Destination option header types. The possible destination option header type and its corresponding *doh-number* value are home-address—201.
dscp *value*	(Optional) Matches a differentiated services codepoint value against the traffic class value in the Traffic Class field of each IPv6 packet header. The acceptable range is from 0 to 63.

flow-label *value*	(Optional) Matches a flow label value against the flow label value in the Flow Label field of each IPv6 packet header. The acceptable range is from 0 to 1048575.
fragments	(Optional) Matches non-initial fragmented packets where the fragment extension header contains a non-zero fragment offset. The **fragments** keyword is an option only if the *operator* [*port-number*] arguments are not specified.
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 name and sequence number, whether the packet was permitted; 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 in the prior 5-minute interval.
log-input	(Optional) Provides the same function as the **log** keyword, except that the logging message also includes the input interface.
mobility	(mobility) Matches IPv6 packets against the mobility extension header within each IPv6 packet header.
mobility-type	(Optional) Matches IPv6 packets against the mobility-type extension header within each IPv6 packet header. Either the *mh-number* or *mh-type* argument must be used with this keyword.
mh-number	(Optional) Integer in the range from 0 to 255 representing an IPv6 mobility header type.
mh-type	(Optional) Mobility header types. Possible mobility header types and their corresponding *mh-number* value are as follows: • 0—bind-refresh • 1—hoti • 2—coti • 3—hot • 4—cot • 5—bind-update • 6—bind-acknowledgment • 7—bind-error
reflect *name*	(Optional) Specifies a reflexive IPvì6 access list. Reflexive IPv6 access lists are created dynamically when an IPv6 packets matches a permit statement that contains the **reflect** keyword. The reflexive IPv6 access list mirrors the permit statement and times out automatically when no IPv6 packets match the permit statement. Reflexive IPv6 access lists can be applied to the TCP, UDP, SCTP, and ICMP for IPv6 packets.
timeout *value*	(Optional) Interval of idle time (in seconds) after which a reflexive IPv6 access list times out. The acceptable range is from 1 to 4294967295. The default is 180 seconds.
routing	(Optional) Matches source-routed packets against the routing extension header within each IPv6 packet header.

routing-type	(Optional) Matches IPv6 packets against the routing-type extension header within each IPv6 packet header. The *routing-number* argument must be used with this keyword.
routing-number	Integer in the range from 0 to 255 representing an IPv6 routing header type. Possible routing header types and their corresponding *routing-number* value are as follows: • 0—Standard IPv6 routing header • 2—Mobile IPv6 routing header
sequence *value*	(Optional) Specifies the sequence number for the access list statement. The acceptable range is from 1 to 4294967295.
time-range *name*	(Optional) Specifies the time range that applies to the permit statement. The name of the time range and its restrictions are specified by the **time-range** and **absolute** or **periodic** commands, respectively.
icmp-type	(Optional) Specifies an ICMP message type for filtering ICMP packets. ICMP packets can be filtered by ICMP message type. The ICMP message type can be a number from 0 to 255, some of which include the following predefined strings and their corresponding numeric values: • 144—dhaad-request • 145—dhaad-reply • 146—mpd-solicitation • 147—mpd-advertisement
icmp-code	(Optional) Specifies an ICMP message code for filtering ICMP packets. 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) Specifies an ICMP message name for filtering ICMP packets. ICMP packets can be filtered by an ICMP message name or ICMP message type and code. The possible names are listed in the "Usage Guidelines" section.
ack	(Optional) For the TCP protocol only: acknowledgment (ACK) bit set.
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.
fin	(Optional) For the TCP protocol only: Fin bit set; no more data from sender.
neq {*port* | *protocol*}	(Optional) Matches only packets that are not on a given port number.
psh	(Optional) For the TCP protocol only: Push function bit set.
range {*port* | *protocol*}	(Optional) Matches only packets in the range of port numbers.
rst	(Optional) For the TCP protocol only: Reset bit set.
syn	(Optional) For the TCP protocol only: Synchronize bit set.
urg	(Optional) For the TCP protocol only: Urgent pointer bit set.

Command Default No IPv6 access list is defined.

Command Modes IPv6 access list configuration

Command History

Release	Modification
12.0(23)S	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.
12.4(2)T	The *icmp-type* argument was enhanced. The **dest-option-type**, **mobility**, **mobility-type**, and **routing-type** keywords were added. The *doh-number*, *doh-type*, *mh-number*, *mh-type*, and *routing-number* arguments 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.
12.2(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 introduced on Cisco ASR 1000 series routers.
12.4(20)T	The **auth** keyword was added.
12.2(33)SRE	This command was modified. It was implemented into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines The **permit** (IPv6) command is similar to the **permit** (IP) command, except that it is IPv6-specific.

Use the **permit** (IPv6) command following the **ipv6 access-list** command to define the conditions under which a packet passes the access list or to define the access list as a reflexive access list.

Specifying IPv6 for the *protocol* argument matches against the IPv6 header of the packet.

By default, the first statement in an access list is number 10, and the subsequent statements are incremented by 10.

You can add **permit**, **deny**, **remark**, or **evaluate** statements to an existing access list without retyping the entire list. To add a new statement anywhere other than at the end of the list, create a new statement with an appropriate entry number that falls between two existing entry numbers to indicate where it belongs.

In Cisco IOS Release 12.2(2)T or later releases, 12.0(21)ST, and 12.0(22)S, IPv6 access control lists (ACLs) are defined and their deny and permit conditions are set by using the **ipv6 access-list** command with the **deny** and **permit** keywords in global configuration mode. In Cisco IOS Release 12.0(23)S or later releases, IPv6 ACLs are defined by using the **ipv6 access-list** command in global configuration mode and their permit and deny conditions are set by using the **deny** and **permit** commands in IPv6 access list configuration mode. Refer to the **ipv6 access-list** command for more information on defining IPv6 ACLs.

Note In Cisco IOS Release 12.0(23)S or later releases, every IPv6 ACL has implicit **permit icmp any any nd-na**, **permit icmp any any nd-ns**, and **deny ipv6 any any** statements as its last match conditions. (The former two match conditions allow for ICMPv6 neighbor discovery.) An IPv6 ACL must contain at least one entry for the implicit **deny ipv6 any any** statement to take effect.

The IPv6 neighbor discovery process makes use of the IPv6 network layer service; therefore, by default,

IPv6 ACLs implicitly allow IPv6 neighbor discovery packets to be sent and received on an interface. In IPv4, the Address Resolution Protocol (ARP), which is equivalent to the IPv6 neighbor discovery process, makes use of a separate data link layer protocol; therefore, by default, IPv4 ACLs implicitly allow ARP packets to be sent and received on an interface.

Both the *source-ipv6-prefix*/*prefix-length* and *destination-ipv6-prefix*/*prefix-length* arguments are used for traffic filtering (the source prefix filters traffic based upon the traffic source; the destination prefix filters traffic based upon the traffic destination).

Note IPv6 prefix lists, not access lists, should be used for filtering routing protocol prefixes.

The **fragments** keyword is an option only if the *operator* [*port-number*] arguments are not specified.

The following is a list of ICMP message names:

- beyond-scope
- destination-unreachable
- echo-reply
- echo-request
- header
- hop-limit
- mld-query
- mld-reduction
- mld-report
- nd-na
- nd-ns
- next-header
- no-admin
- no-route
- packet-too-big
- parameter-option
- parameter-problem
- port-unreachable
- reassembly-timeout
- renum-command
- renum-result
- renum-seq-number
- router-advertisement
- router-renumbering
- router-solicitation
- time-exceeded
- unreachable

Defining Reflexive Access Lists

To define an IPv6 reflexive list, a form of session filtering, use the **reflect** keyword in the **permit** (IPv6) command. The **reflect** keyword creates an IPv6 reflexive access list and triggers the creation of entries in the reflexive access list. The **reflect** keyword must be an entry (condition statement) in an IPv6 access list.

Note For IPv6 reflexive access lists to work, you must nest the reflexive access list using the **evaluate** command.

If you are configuring IPv6 reflexive access lists for an external interface, the IPv6 access list should be one that is applied to outbound traffic.

If you are configuring an IPv6 reflexive access list for an internal interface, the IPv6 access list should be one that is applied to inbound traffic.

IPv6 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 IPv6 access list, the packet is also evaluated against the IPv6 reflexive permit entry.

As with all IPv6 access list entries, the order of entries is important, because they are evaluated in sequential order. When an IPv6 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 that the packet belongs to a session in progress). The temporary entry specifies criteria that permit traffic into your network only for the same session.

Characteristics of Reflexive Access List Entries

The **permit** (IPv6) command with the **reflect** keyword enables the creation of temporary entries in the same IPv6 reflexive access list that was defined by the **permit** (IPv6) command. The temporary entries are created when an IPv6 packet exiting your network matches the protocol specified in the **permit** (IPv6) 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 that 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 that 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.

- IPv6 traffic entering your internal network will be evaluated against the entry, until the entry expires. If an IPv6 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 configured length of time (the timeout period), the entry will expire.

Examples

The following example configures two IPv6 access lists named OUTBOUND and INBOUND and applies both access lists to outbound and inbound traffic on Ethernet interface 0. The first and second permit entries in the OUTBOUND list permit all TCP and UDP packets from network 2001:ODB8:0300:0201::/64 to exit out of Ethernet interface 0. The entries also configure the temporary IPv6 reflexive access list named REFLECTOUT to filter returning (incoming) TCP and UDP packets on Ethernet interface 0. The first deny entry in the OUTBOUND list keeps all packets from the network FEC0:0:0:0201::/64 (packets that have the site-local prefix FEC0:0:0:0201 as the first 64 bits of their source IPv6 address) from exiting out of Ethernet interface 0. The third permit entry in the OUTBOUND list permits all ICMP packets to exit out of Ethernet interface 0.

The permit entry in the INBOUND list permits all ICMP packets to enter Ethernet interface 0. The **evaluate** command in the list applies the temporary IPv6 reflexive access list named REFLECTOUT to inbound TCP and UDP packets on Ethernet interface 0. When outgoing TCP or UDP packets are permitted on Ethernet interface 0 by the OUTBOUND list, the INBOUND list uses the REFLECTOUT list to match (evaluate) the returning (incoming) TCP and UDP packets. Refer to the **evaluate** command for more information on nesting IPv6 reflexive access lists within IPv6 ACLs.

```
ipv6 access-list OUTBOUND
 permit tcp 2001:0DB8:0300:0201::/64 any reflect REFLECTOUT
 permit udp 2001:0DB8:0300:0201::/64 any reflect REFLECTOUT
 deny FEC0:0:0:0201::/64 any
 permit icmp any any

ipv6 access-list INBOUND
 permit icmp any any
 evaluate REFLECTOUT

interface ethernet 0
 ipv6 traffic-filter OUTBOUND out
 ipv6 traffic-filter INBOUND in
```

Note Given that a **permit any any** statement is not included as the last entry in the OUTBOUND or INBOUND access list, only TCP, UDP, and ICMP packets will be permitted out of and in to Ethernet interface 0 (the implicit deny all condition at the end of the access list denies all other packet types on the interface).

The following example shows how to allow the matching of any UDP traffic. The authentication header may be present.

```
permit udp any any sequence 10
```

The following example shows how to allow the matching of only TCP traffic if the authentication header is also present.

```
permit tcp any any auth sequence 20
```

The following example shows how to allow the matching of any IPv6 traffic where the authentication header is present.

```
permit ahp any any sequence 30
```

Related Commands

Command	Description
ipv6 access-list	Defines an IPv6 access list and enters IPv6 access list configuration mode.
ipv6 traffic-filter	Filters incoming or outgoing IPv6 traffic on an interface.
deny (IPv6)	Sets deny conditions for an IPv6 access list.
evaluate (IPv6)	Nests an IPv6 reflexive access list within an IPv6 access list.
show ipv6 access-list	Displays the contents of all current IPv6 access lists.

ping

To diagnose basic network connectivity on AppleTalk, ATM, Connectionless Network Service (CLNS), DECnet, IP, Novell IPX, or source-route bridging (SRB) networks, use the **ping** command in user EXEC or privileged EXEC mode.

ping [[*protocol* [**tag**] {*host-name* | *system-address*}]

Syntax Description

protocol	(Optional) Protocol keyword, either **appletalk**, **atm**, **clns**, **decnet**, **ipx**, or **srb**. If a protocol is not specified, a basic ping will be sent using IP (IPv4). For extended options for ping over IP, see the documentation for the **ping ip** command. The **ping atm interface atm**, **ping ip**, **ping ipv6**, **ping sna**, and **ping vrf** commands are documented separately.
tag	(Optional) Specifies a tag encapsulated IP (tagIP) ping.
host-name	Hostname of the system to ping. If a *host-name* or *system-address* is not specified at the command line, it will be required in the **ping** system dialog.
system-address	Address of the system to ping. If a *host-name* or *system-address* is not specified at the command line, it will be required in the **ping** system dialog.

Command Default

This command has no default values.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.0(7)T	The **ping sna** command was introduced.
12.1(12c)E	The **ping vrf** command was introduced.
12.2(2)T	Support for the IPv6 protocol was added.
12.2(13)T	The **atm** protocol keyword was added. The following keywords were removed because the Apollo Domain, Banyan VINES, and XNS protocols are no longer supported in Cisco IOS software: • **apollo** • **vines** • **xns**
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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
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

The **ping** command sends an echo request packet to an address then waits for a reply. Ping output can help you evaluate path-to-host reliability, delays over the path, and whether the host can be reached or is functioning. For example, the **ping clns** command sends International Organization for Standardization (ISO) CLNS echo packets to test the reachability of a remote router over a connectionless Open System Interconnection (OSI) network.

If you enter the **ping** command without any keywords or argument values, an interactive system dialog prompts you for the additional syntax appropriate to the protocol you specify. (See the "Examples" section.)

To exit the interactive ping dialog before responding to all the prompts, type the escape sequence. The default escape sequence is **Ctrl**-**^**, **X** (Simultaneously press and release the **Ctrl**, **Shift**, and **6** keys and then press the **X** key). The escape sequence will vary depending on your line configuration. For example, another commonly used escape sequence is **Ctrl**-**c**.

Table 39 describes the test characters sent by the **ping** facility.

Table 39 ping Test Characters

Character	Description
!	Each exclamation point indicates receipt of a reply.
.	Each period indicates that the network server timed out while waiting for a reply.
U	A destination unreachable error protocol data unit (PDU) was received.
C	A reply packet does not validate the reply data, and hence is marked "Corrupted". **Note** This character will only appear if the "validate" option is selected in the ping request.
I	User interrupted test.
M	A destination unreachable error protocol data unit (PDU) was received (Type 3) MTU required but DF bit set (code 4) with the "Next-Hop MTU" set to a non-zero value. If the "Next-hop MTU" is zero then 'U' is printed.
?	Unknown packet type.
&	Packet lifetime exceeded.

Note Not all protocols require hosts to support pings. For some protocols, the pings are Cisco defined and can be answered only by another Cisco router.

The availability of protocol keywords depends on what protocols are enabled on your system.

Issuing the **ping** command in user EXEC mode will generally offer fewer syntax options than issuing the **ping** command in privileged EXEC mode.

Examples

After you enter the **ping** command in privileged EXEC mode, the system prompts you for a protocol keyword. The default protocol is IP.

If you enter a hostname or address on the same line as the **ping** command, the default action is taken as appropriate for the protocol type of that name or address.

The following example is sample dialog from the **ping** command using default values. The specific dialog varies somewhat from protocol to protocol.

```
Router# ping

Protocol [ip]:
Target IP address: 192.168.7.27

Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.7.27, timeout is 2 seconds:
!!!!!
Success rate is 100 percent, round-trip min/avg/max = 1/2/4 ms
```

Table 40 describes the significant fields shown in the display.

Table 40 ping Field Descriptions for IP

Field	Description
Protocol [ip]:	Prompt for a supported protocol. Default: **ip**.
Target IP address:	Prompt for the IP address or hostname of the destination node you plan to ping. If you have specified a supported protocol other than IP, enter an appropriate address for that protocol here. Default: none.
Repeat count [5]:	Number of ping packets that will be sent to the destination address. Default: 5.
Datagram size [100]:	Size of the ping packet (in bytes). Default: 100 bytes.
Timeout in seconds [2]:	Timeout interval. Default: 2 (seconds).
Extended commands [n]:	Specifies whether a series of additional commands appears.
Sweep range of sizes [n]:	Allows you to vary the sizes of the echo packets being sent. This capability is useful for determining the minimum sizes of the maximum transmission units (MTUs) configured on the nodes along the path to the destination address. Packet fragmentation contributing to performance problems can then be reduced.
!!!!!	Each exclamation point (!) indicates receipt of a reply. A period (.) indicates that the network server timed out while waiting for a reply. Other characters may appear in the ping output display, depending on the protocol type.

Table 40 ping Field Descriptions for IP (continued)

Field	Description
Success rate is 100 percent	Percentage of packets successfully echoed back to the router. Anything less than 80 percent is usually considered problematic.
round-trip min/avg/max = 1/2/4 ms	Round-trip travel time intervals for the protocol echo packets, including minimum/average/maximum (in milliseconds).

The following example verifies connectivity to the neighboring ATM device for the ATM permanent virtual circuit (PVC) with the virtual path identifier (VPI)/virtual channel identifier (VCI) value 0/16:

```
Router# ping

Protocol [ip]:atm
ATM Interface:atm1/0
VPI value [0]:
VCI value [1]:16
Loopback - End(0), Segment(1) [0]:1
Repeat Count [5]:
Timeout [2]:
Type escape sequence to abort.
Sending 5, 53-byte segment OAM echoes, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Table 41 describes the default **ping** fields shown in the display.

Table 41 ping Field Descriptions for ATM

Field	Description
Protocol [ip]:	Prompt for a supported protocol. Default: **ip**.
ATM Interface:	Prompt for the ATM interface.
VPI value [0]:	Prompt for the virtual path identifier. Default: 0.
VCI value [1]:	Prompt for the virtual channel identifier. Default:1.
Loopback - End(0), Segment(1) [0]:	Prompt to specify end loopback, which verifies end-to-end PVC integrity, or segment loopback, which verifies PVC integrity to the neighboring ATM device. Default: segment loopback.
Repeat Count [5]:	Number of ping packets that will be sent to the destination address. Default: 5.
Timeout [2]:	Timeout interval. Default: 2 (seconds).
!!!!!	Each exclamation point (!) indicates receipt of a reply. A period (.) indicates that the network server timed out while waiting for a reply. Other characters may appear in the ping output display, depending on the protocol type.

Table 41 ping Field Descriptions for ATM (continued)

Field	Description
Success rate is 100 percent	Percentage of packets successfully echoed back to the router. Anything less than 80 percent is usually considered problematic.
round-trip min/avg/max = 1/1/1 ms	Round-trip travel time intervals for the protocol echo packets, including minimum/average/maximum (in milliseconds).

Related Commands

Command	Description
ping atm interface atm	Tests the connectivity of a specific PVC.
ping ip	Tests network connectivity on IP networks.
ping ipv6	Tests the connection to a remote host on the network using IPv6.
ping sna	Tests network integrity and timing characteristics over an SNA Switching network.
ping vrf	Tests the connection in the context of a specific VPN (VRF).

ping ipv6

To diagnose basic network connectivity when using IPv6, use the **ping IPv6** command in user EXEC or privileged EXEC mode.

ping ipv6 *ipv6-address* [**data** *hex-data-pattern* | **repeat** *repeat-count* | **size** *datagram-size* | **source** [**async** | **bvi** | **ctunnel** | **dialer** | **ethernet** | **fastEthernet** | **gigabitEthernet** | **loopback** | **mfr** | **multilink** | **null** | **port-channel** | **tunnel** | **virtual-template** | *source-address* | **xtagatm**] | **timeout** *seconds* | **verbose**]

Syntax Description

ipv6-address	The address or hostname of the IPv6 host to be pinged. This address or hostname must be in the form documented in RFC 2373, where the address is specified in hexadecimal using 16-bit values between colons.
data	(Optional) Specifies the data pattern.
hex-data-pattern	(Optional) Range is from 0 to FFFF.
repeat	(Optional) Specifies the number of pings sent. The default is 5.
repeat-count	(Optional) Range is from 1 to 2147483647.
size	(Optional) Specifies the datagram size. Datagram size is the number of bytes in each ping.
datagram-size	(Optional) Range is from 48 to 18024.
source	(Optional) Specifies the source address or name.
async	(Optional) Asynchronous interface.
bvi	(Optional) Bridge-Group Virtual Interface.
ctunnel	(Optional) CTunnel interface.
dialer	(Optional) Dialer interface.
ethernet	(Optional) Ethernet IEEE 802.3.
fastEthernet	(Optional) FastEthernet IEEE 802.3.
gigabitEthernet	(Optional) GigabitEthernet IEEE 802.3z.
loopback	(Optional) Loopback interface.
mfr	(Optional) Multilink frame relay (MFR) bundle interface.
multilink	(Optional) Multilink-group interface.
null	(Optional) Null interface.
port-channel	(Optional) Ethernet channel of interfaces.
tunnel	(Optional) Tunnel interface.
virtual-template	(Optional) Virtual template interface.
source-address	(Optional) Source IPv6 address or name.
xtagatm	(Optional) Extended Tag ATM interface.
timeout	(Optional) Specifies the timeout interval in seconds. The default is 2 seconds.
seconds	(Optional) Range is from 0 to 3600.
verbose	(Optional) Displays the verbose output.

Command Modes

User EXEC
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(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.
12.2(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 introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The user-level ping feature provides a basic ping facility for users that do not have system privileges. This feature allows the Cisco IOS software to perform the simple default ping functionality for a number of protocols.

The ping program sends an echo request packet to an address, then awaits a reply. Ping output can help you evaluate path-to-host reliability, delays over the path, and whether the host can be reached or is functioning.

If the system cannot map an address for a hostname, it returns an "%Unrecognized host or address, or protocol not running" message.

To abnormally terminate a ping session, type the escape sequence—by default, Ctrl-^ X. You type the default by simultaneously pressing and releasing the Ctrl, Shift, and 6 keys, and then pressing the X key.

Caution When the **timeout** keyword is used with the *seconds* argument set to 0, an immediate timeout occurs, which causes a flood ping. Use the **timeout 0** parameter with caution, because you may receive replies only from immediately adjacent routers depending on router and network use, distance to the remote device, and other factors.

Table 42 describes the characters displayed by the ping facility in IPv6.

Table 42 ping Test Characters (IPv6)

!	Each exclamation point indicates receipt of a reply.
.	Each period indicates that the network server timed out while waiting for a reply.
?	Unknown error.
@	Unreachable for unknown reason.
A	Administratively unreachable. Usually, this output indicates that an access list is blocking traffic.
B	Packet too big.
H	Host unreachable.
N	Network unreachable (beyond scope).

Table 42 ping Test Characters (IPv6) (continued)

P	Port unreachable.
R	Parameter problem.
S	Source address failed ingress/egress policy.
T	Time exceeded.
U	No route to host.
X	Reject route to destination.

Note Not all protocols require hosts to support pings. For some protocols, the pings are Cisco-defined and are answered only by another Cisco router.

When the **ping ipv6** command is enabled, the router attempts to resolve hostnames into IPv6 addresses before trying to resolve them into IPv4 addresses, so if a hostname resolves to both an IPv6 and an IPv4 address and you specifically want to use the IPv4 address, use the **ping** (IPv4) command.

Examples

The following user EXEC example shows sample output for the **ping ipv6** command:

```
Router# ping ipv6 2001:0DB8::3/64

Target IPv6 address: 2001:0DB8::3/64
Repeat count [5]:
Datagram size [100]:48
Timeout in seconds [2]:
Extended commands? [no]: yes
UDP protocol? [no]:
Verbose? [no]:
Precedence [0]:
DSCP [0]:
Include hop by hop option? [no]:yes
Include destination option? [no]:y
% Using size of 64 to accommodate extension headers
Sweep range of sizes? [no]:y
Sweep min size [100]: 100
Sweep max size [18024]: 150
Sweep interval [1]: 5
Sending 55, [100..150]-byte ICMP Echos to 2001:0DB8::3/64, timeout is 2 seconds:
Success rate is 100 percent
round-trip min/avg/max = 2/5/10 ms
```

Table 43 describes the default **ping ipv6** fields shown in the display.

Table 43 ping ipv6 Field Descriptions

Field	Description
Target IPv6 address:	Prompts for the IPv6 address or host name of the destination node you plan to ping. Default: none.
Repeat count [5]:	Number of ping packets that will be sent to the destination address. Default: 5.
Datagram size [100]:	Size of the ping packet (in bytes). Default: 100 bytes.

Table 43 ping ipv6 Field Descriptions (continued)

Field	Description
Timeout in seconds [2]:	Timeout interval (in seconds). Default: 2.
Extended commands [no]:	Specifies whether a series of additional commands appears. Default: no. In an IPv6 dialog for the **ping IPv6** command, entering yes in the Extended commands field displays the UDP protocol?, Verbose, Priority, and Include extension headers? fields.
UDP protocol? [no]:	Specifies UDP packets or ICMPv6 packets. Default: no (ICMP packets are sent).
Verbose? [no]:	Enables verbose output.
Precedence [0]:	Sets precedence in the IPv6 header. The range is from 0 to 7.
DSCP [0]:	Sets Dynamic Host Configuration Protocol (DSCP) in the IPv6 header. The range is from 0 to 63. DSCP appears only if the precedence option is not set, because precedence and DSCP are two separate ways of viewing the same bits in the header.
Include hop by hop option? [no]:	The IPv6 hop-by-hop option is included in the outgoing echo request header, requiring the ping packet to be examined by each node along the path and therefore not be fast-switched or Cisco Express Forwarding-switched. This function may help with debugging network connectivity, especially switching problems. **Note** A Cisco router also includes the hop-by-hop option in the returned echo reply, so the packets should be process-switched rather than fast-switched or Cisco Express Forwarding-switched on the return path also. Non-Cisco routers likely do not have this option in their echo reply; therefore, if the echo request with hop-by-hop option arrives at the destination but the echo reply does not come back and the destination is not a Cisco router, a fast-path issue may exist in an intermediate router.
Include destination option? [no]:	Includes an IPv6 destination option in the outgoing echo request header.
Sweep range of sizes? [no]:	Allows you to vary the sizes of the echo packets being sent. This capability is useful for determining the minimum sizes of the maximum transmission units (MTUs) configured on the nodes along the path to the destination address. Packet fragmentation contributing to performance problems can then be reduced.
Sweep min size [100]: Sweep max size [18024]: Sweep interval [1]:	Options that appear if "Sweep range of sizes?" option is enabled. • Sweep min size—Defaults to the configured "Datagram size" parameter and will override that value if specified. • Sweep Interval—The size of the intervals between the "Sweep min size" and "Sweep max size" parameters. For example, min of 100 max of 150 with an interval of 5 means packets sent are of 100, 105, 110, ..., 150 bytes in size.

Table 43 ping ipv6 Field Descriptions (continued)

Field	Description
Sending 55, [100..150]-byte ICMP Echos to ...	Minimum and maximum sizes and interval as configured in "Sweep range of sizes" options. Sizes are reported if the ping fails (but not if it succeeds, unless the verbose option is enabled).
Success rate is 100 percent	Percentage of packets successfully echoed back to the router. Anything less than 80 percent is usually considered problematic.
round-trip min/avg/max = 2/5/10 ms	Round-trip minimum, average, and maximum time intervals for the protocol echo packets (in milliseconds).

ping vrf

To test a connection in the context of a specific VPN connection, use the **ping vrf** command in user EXEC or privileged EXEC mode.

ping vrf *vrf-name* [**tag**] [*connection*] *target-address* [*connection-options*]

Syntax Description

vrf-name	The name of the VPN (VRF context).
tag	(Optional) Specifies a tag encapsulated IP (tagIP) ping.
connection	(Optional) Connection options include **atm**, **clns**, **decnet**, **ip**, **ipv6**, **ipx**, **sna**, or **srb**. The default is **ip**.
target-address	The destination ID for the ping operation. Usually, this is the IPv4 address of the host. For example, the target for an IPv4 ping in a VRF context would be the IPv4 address or domain name of the target host. The target for an IPv6 ping in a VRF context would be the IPv6 prefix or domain name of the target host. • If the target address is not specified, the CLI will enter the interactive dialog for ping.
connection-options	(Optional) Each connection type may have its own set of connection options. For example, connection options for IPv4 are **source**, **df-bit**, and **timeout**. See the appropriate **ping** command documentation for details.

Command Default

The default connection type for ping is IPv4.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.1(12c)E, 12.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
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.

Usage Guidelines

A VPN routing and forwarding (VRF) instance is used to identify a VPN. To check if a configured VRF is working, you can use the **ping vrf** command.

When attempting to ping from a provider edge (PE) router to a customer edge (CE) router, or from a PE router to PE router, the standard **ping** command will not usually work. The **ping vrf** command allows you to ping the IP addresses of LAN interfaces on CE routers.

If you are on a PE router, be sure to indicate the specific VRF (VPN) name, as shown in the "Examples" section.

If all required information is not provided at the command line, the system will enter the interactive dialog (extended mode) for ping.

Examples

In the following example, the target host in the domain 209.165.201.1 is pinged (using IP/ICMP) in the context of the "CustomerA" VPN connection.

```
Router# ping vrf CustomerA 209.165.201.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.201.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 176/264/576 ms
```

Pressing the Enter key before providing all of the required options will begin the interactive dialog for ping. In the following example, the interactive dialog is started after the "ip" protocol is specified, but no address is given:

```
Router# ping vrf CustomerB ip

Target IP address: 209.165.200.225
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface:
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]: Record
Number of hops [ 9 ]:
Loose, Strict, Record, Timestamp, Verbose[RV]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.225, timeout is 2 seconds:
Packet has IP options:  Total option bytes= 39, padded length=40
 Record route: <*>
   (0.0.0.0)
   (0.0.0.0)
   (0.0.0.0)
   (0.0.0.0)
   (0.0.0.0)
   (0.0.0.0)
   (0.0.0.0)
   (0.0.0.0)
   (0.0.0.0)
 .
 .
 .
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
```

The following example shows the various options for IP in the **ping vrf** command:

```
Router# show parser dump exec | include ping vrf

1 ping vrf <string>
1 ping vrf <string> ip <string>
1 ping vrf <string> ip (interactive)
1 ping vrf <string> ip <string>
1 ping vrf <string> ip <string> source <address>
1 ping vrf <string> ip <string> source <interface>
1 ping vrf <string> ip <string> repeat <1-2147483647>
```

```
1 ping vrf <string> ip <string> size Number
1 ping vrf <string> ip <string> df-bit
1 ping vrf <string> ip <string> validate
1 ping vrf <string> ip <string> data <0-65535>
1 ping vrf <string> ip <string> timeout <0-3600>
1 ping vrf <string> ip <string> verbose
1 ping vrf <string> ip <string> data <0-65535>
1 ping vrf <string> ip <string> timeout <0-3600>
1 ping vrf <string> tag
1 ping vrf <string> atm
1 ping vrf <string> ipv6
1 ping vrf <string> appletalk
1 ping vrf <string> decnet
1 ping vrf <string> clns
1 ping vrf <string> ipx
1 ping vrf <string> sna
1 ping vrf <string> srb
```

Related Commands

Command	Description
ping	Diagnoses basic network connectivity to a specific host.
ping atm interface atm	Tests the connectivity of a specific PVC.
ping ip	Tests the connection to a remote host on the network using IPv4.
ping ipv6	Tests the connection to a remote host on the network using IPv6.
ping sna	Tests network integrity and timing characteristics over an SNA Switching network.

platform ipv6 acl fragment hardware

To permit or deny fragments at hardware, use the **platform ipv6 acl fragment hardware** command in global configuration mode. To reset the IPv6 fragment handling to bridged mode, use the **no** form of this command.

platform ipv6 acl fragment hardware {**forward** | **drop**}

no platform ipv6 acl fragment hardware {**forward** | **drop**}

Syntax Description

forward	Forwards the IPv6 fragments in the hardware.
drop	Drops the IPv6 fragments in the hardware.

Command Default

The **no** form of this command is the default behavior.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.

Usage Guidelines

The PFC3A, PFC3B, and PFC3BXL are unable to handle IPv6 fragments in hardware, and all IPv6 fragments are handled in software. This could result in high CPU if your traffic includes a large amount of IPv6 fragments. This limitation is handled in the PFC3C hardware. The **platform ipv6 acl fragment hardware** command provides a software workaround for the PFC3A, PFC3B, and PFC3BXL by specifying either to permit or drop all IPv6 fragments in hardware.

Note When you enter the **drop** keyword, a small portion of the packets is leaked to the software (for ICMP message generation) and forwarded in software.

The **platform ipv6 acl fragment hardware** command overrides the following actions:

- Any ACE in the IPv6 filter (ACL) that contains the **fragment** keyword. If the ACE in the ACL contains the **fragment** keyword, the associated action (**permit** | **deny** | **log**) is not taken, and the action (**permit** | **drop**) specified by the **platform ipv6 acl fragment hardware** command is taken.
- Any IPv6 ACL that contains ACEs that implicitly permit IPv6 fragments; for example, permit ACEs that contain Layer 4 ports to implicitly permit fragments only.
- If the IPv6 fragment hits the implicit **deny any any** ACE added at the end of the ACL, the IPv6 fragment will not get hit.

Examples

This example shows how to forward the IPv6 fragments at hardware:

```
Router(config)# platform ipv6 acl fragment hardware forward
```

This example shows how to drop the IPv6 fragments at hardware:

```
Router(config)# platform ipv6 acl fragment hardware drop
```

platform ipv6 acl icmp optimize neighbor-discovery

To optimize ternary content addressable memory (TCAM) support for IPv6 access lists (ACLs), use the **platform ipv6 acl icmp optimize neighbor-discovery** command in global configuration mode. To disable optimization of TCAM support for IPv6 ACLs, use the **no** form of this command.

platform ipv6 acl icmp optimize neighbor-discovery

no platform ipv6 acl icmp optimize neighbor-discovery

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	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

Note Use this command under the direction of the Cisco Technical Assistance Center only.

When you enable optimization of the TCAM support for IPv6 ACLs, the global Internet Control Message Protocol version 6 (ICMPv6) neighbor-discovery ACL at the top of the TCAM is programmed to permit all ICMPv6 neighbor-discovery packets. Enabling optimization prevents the addition of ICMPv6 access control entries (ACEs) at the end of every IPv6 security ACL, reducing the number of TCAM resources being used. Enabling this command reprograms IPv6 ACLs on all interfaces.

Note The ICMPv6 neighbor-discovery ACL at the top of the TCAM takes precedence over security ACLs for ICMP neighbor-discovery packets that you have configured, but has no effect if you have a bridge/deny that overlaps with the global ICMP ACL.

Examples

This example shows how to optimize TCAM support for IPv6 ACLs:

```
Router(config)# platform ipv6 acl icmp optimize neighbor-discovery
```

This example shows how to disable optimization of TCAM support for IPv6 ACLs:

```
Router(config)# no platform ipv6 acl icmp optimize neighbor-discovery
```

platform ipv6 acl punt extension-header

To enable processing of IPv6 packets with extension headers in software on the RP, use the **platform ipv6 acl punt extension-header** command in global configuration mode. To disable processing of IPv6 packets with extension headers in software on the RP, use the **no** form of this command.

platform ipv6 acl punt extension-header

no platform ipv6 acl punt extension-header

Syntax Description

This command has no arguments or keywords.

Command Default

IPv6 packets with extension headers are processed in software.

Command Modes

Global configuration mode

Command History

Release	Modification
12.2(33)SXH7	This command was introduced on the Supervisor Engine 720.

Usage Guidelines

If your IPv6 traffic does not specify a Layer 4 protocol, software processing of IPv6 packets with extension headers is unnecessary. If your IPv6 traffic specifies a Layer 4 protocol, you can enter the **platform ipv6 acl punt extension-header** global configuration command to enable software processing of IPv6 packets with extension headers.

Examples

This example shows how to enable processing of IPv6 packets with extension headers in software on the RP:

```
Router(config)# platform ipv6 acl punt extension-header
Router(config)#
```

This example shows how to disable processing of IPv6 packets with extension headers in software on the RP:

```
Router(config)# no platform ipv6 acl punt extension-header
Router(config)#
```

poison-reverse (IPv6 RIP)

To configure the poison reverse processing of IPv6 Routing Information Protocol (RIP) router updates, use the **poison-reverse** command in router configuration mode. To disable the poison reverse processing of IPv6 RIP updates, use the **no** form of this command.

poison-reverse

no poison-reverse

Syntax Description

This command has no keywords or arguments

Command Default

Poison reverse is not configured.

Command Modes

Router configuration

Command History

Release	Modification
12.2(2)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 Release 12.2(14)S.
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.
12.2(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 configures poison reverse processing of IPv6 RIP router updates. When poison reverse is configured, routes learned via RIP are advertised out the interface over which they were learned, but with an unreachable metric.

If both poison reverse and split horizon are configured, then simple split horizon behavior (suppression of routes out of the interface over which they were learned) is replaced by poison reverse behavior.

Examples

The following example configures poison reverse processing for the IPv6 RIP routing process named cisco:

```
Router(config)# ipv6 router rip cisco
Router(config-rtr)# poison-reverse
```

Related Commands

Command	Description
split-horizon (IPv6 RIP)	Configures split horizon processing of IPv6 RIP router updates.

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**
15.1(2)T	Support for IPv6 was added.

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.

port (dial peer)

To associate a dial peer with a specific voice port, use the **port** command in dial peer configuration mode. To cancel this association, use the **no** form of this command.

Cisco 1750 and Cisco 3700 Series

port *slot-number*/*port*

no port *slot-number*/*port*

Cisco 2600 Series, Cisco 3600 Series, and Cisco 7200 Series

port {*slot-number*/*subunit-number*/*port* | *slot*/*port*:*ds0-group-number*}

no port {*slot-number*/*subunit-number*/*port* | *slot*/*port*:*ds0-group-number*}

Cisco AS5300 and Cisco AS5800

port *controller-number*:**D**

no port *controller-number*:**D**

Cisco uBR92x Series

port *slot*/*subunit*/*port*

no port *slot*/*subunit*/*port*

Syntax Description

Cisco 1750 and Cisco 3700 Series

slot-number	Number of the slot in the router in which the voice interface card (VIC) is installed. Valid entries are from 0 to 2, depending on the slot in which the VIC has been installed.
port	Voice port number. Valid entries are 0 and 1.

Cisco 2600 Series, Cisco 3600 Series, and Cisco 7200 Series

slot-number	Number of the slot in the router in which the VIC is installed. Valid entries are from 0 to 3, depending on the slot in which it has been installed.
subunit-number	Subunit on the VIC in which the voice port is located. Valid entries are 0 and 1.
port	Voice port number. Valid entries are 0 and 1.
slot	Router location in which the voice port adapter is installed. Valid entries are 0 and 3.
port	Voice interface card location. Valid entries are 0 and 3.
ds0-group-number	The DS0 group number. Each defined DS0 group number is represented on a separate voice port. This allows you to define individual DS0s on the digital T1/E1 card.

Cisco AS5300

controller-number	The T1 or E1 controller.
:D	Indicates the D channel associated with the ISDN PRI.

Cisco uBR92x series

slot/*subunit*/*port*	The analog voice port. Valid entries for the *slot*/*subunit*/*port* are as follows: • *slot*—A router slot in which a voice network module (NM) is installed. Valid entries are router slot numbers for the particular platform. • *subunit*—A VIC in which the voice port is located. Valid entries are 0 and 1. (The VIC fits into the voice network module.) • *port*—An analog voice port number. Valid entries are 0 and 1.

Command Default

No port is configured.

Command Modes

Dial peer configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
11.3(3)T	This command was implemented on the Cisco 2600 series.
11.3(1)MA	This command was implemented on the Cisco MC3810.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T and implemented on the Cisco AS5300.
12.0(4)T	This command was implemented on the Cisco uBR924.
12.0(7)T	This command was implemented on the Cisco AS5800.
12.2(8)T	This command was implemented on the following platforms: Cisco 1751, Cisco 3725, and Cisco 3745.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T. This command does not support the extended echo canceller (EC) feature on the Cisco AS5300 or the Cisco AS5800.
12.4(22)T	Support for IPv6 was added.

Usage Guidelines

This command enables calls that come from a telephony interface to select an incoming dial peer and for calls that come from the VoIP network to match a port with the selected outgoing dial peer.

This command applies only to POTS peers.

Note This command does not support the extended EC feature on the Cisco AS5300.

Examples

The following example associates POTS dial peer 10 with voice port 1, which is located on subunit 0 and accessed through port 0:

```
dial-peer voice 10 pots
 port 1/0/0
```

The following example associates POTS dial peer 10 with voice port 0:D:

```
dial-peer voice 10 pots
 port 0:D
```

The following example associates POTS dial peer 10 with voice port 1/0/0:D (T1 card):

```
dial-peer voice 10 pots
 port 1/0/0:D
```

Related Commands

Command	Description
prefix	Specifies the prefix of the dialed digits for a dial peer.

port (IPv6 RIP)

To configure a specified User Datagram Protocol (UDP) port and multicast address for an IPv6 Routing Information Protocol (RIP) routing process, use the **port** command in router configuration mode. To return the port number and multicast address to their default values, use the **no** form of this command.

port *port-number* **multicast-group** *multicast-address*

no port *port-number* **multicast-group** *multicast-address*

Syntax Description

port-number	The UDP port number. Can be a number from 1 to 65535. Table 44 in the "Usage Guidelines" section lists common UDP services and their port numbers.
multicast-group	Specifies a multicast group.
multicast-address	The address or host name of the multicast group.

Command Default

UDP port 521; multicast address FF02::9

Command Modes

Router configuration

Command History

Release	Modification
12.2(2)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 Release 12.2(14)S.
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.
12.2(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

Two IPv6 RIP routing processes cannot use the same UDP port. If two IPv6 RIP routing processes are configured on the same UDP port, the second process will not start up until the configuration conflict is resolved. Two IPv6 RIP routing processes can use the same multicast address. UDP sources and port numbers are shown in Table 44.

Table 44 Common UDP Services and Their Port Numbers

Service	Port
Domain Name System (DNS)	53
Network File System (NFS)	2049
remote-procedure call (RPC)	111

Table 44 Common UDP Services and Their Port Numbers (continued)

Service	Port
Simple Network Management Protocol (SNMP)	161
Trivial File Transfer Protocol (TFTP)	69

Examples

The following example configures UDP 200 and multicast address FF02::9 for the IPv6 RIP routing process named cisco:

```
Router(config)# ipv6 router rip cisco
Router(config-rtr-rip)# port 200 multicast-group FF02::9
```

port (TACACS+)

To specify the TCP port to be used for TACACS+ connections, use the **port** command in TACACS+ server configuration mode. To remove the TCP port, use the **no** form of this command.

port [*number*]

no port [*number*]

Syntax Description

number	(Optional) Specifies the port where the TACACS+ server receives access-request packets. The range is from 1 to 65535.

Command Default

If no port is configured, port 49 is used.

Command Modes

TACACS+ server configuration (config-server-tacacs)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines

TCP port 49 is used if the *number* argument is not used when using the **port** command.

Examples

The following example shows how to specify TCP port 12:

```
Router (config)# tacacs server server1
Router(config-server-tacacs)# port 12
```

Related Commands

Command	Description
tacacs server	Configures the TACACS+ server for IPv6 or IPv4 and enters TACACS+ server configuration mode.

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** | *listname*}

no ppp accounting

Syntax Description

default	The name of the method list is created with the **aaa accounting** command.
listname	A specified method list.

Command Default

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.
Cisco IOS XE Release 2.6	The *listname* argument was added.

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 list1
```

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 45.
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.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(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.
Cisco IOS XE Release 2.5	This command was updated. It was integrated into Cisco IOS XE Release 2.5.

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 45 lists the protocols used to negotiate PPP authentication.

Table 45 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 ipcp

To configure PPP IP Control Protocol (IPCP) features such as the ability to provide primary and secondary Domain Name Server (DNS) and Windows Internet Naming Service (WINS) server addresses, and the ability to accept any address requested by a peer, use the **ppp ipcp** command in template or interface configuration mode. To disable a PPP IPCP feature, use the **no** form of this command.

ppp ipcp {**accept-address** | **address** {**accept** | **required** | **unique**} | **dns** {*primary-ip-address* [*secondary-ip-address*] [**aaa**] [**accept**] | **accept** | **reject** | **request** [**accept**]} | **header-compression ack** | **ignore-map** | **mask** {*subnet-mask* | **reject** | **request**} | **username unique** | **wins** {*primary-ip-address* [*secondary-ip-address*] [**aaa**] [**accept**] | **accept** | **reject** | **request** [**accept**]}}

no ppp ipcp {**accept-address** | **address** {**accept** | **required** | **unique**} | **dns** | **header-compression ack** | **ignore-map** | **mask** | **predictive** | **username unique** | **wins**}

Syntax Description

accept-address	Accepts any nonzero IP address from the peer.
address	Specifies IPCP IP address options: • **accept**—Accepts any nonzero IPv4 or IPv6 address from the peer. • **required**—Disconnects the peer if no IP address is negotiated. • **unique**—Disconnects the peer if the IP address is already in use.
dns	Specifies DNS options: • *primary-ip-address*—IP address of the primary DNS server. – *secondary-ip-address*—(Optional) IP address of the secondary DNS server. – **aaa**—(Optional) Uses DNS data from the AAA server. – **accept**—(Optional) Specifies that any nonzero DNS address will be accepted. • **accept**—Specifies that any nonzero DNS address will be accepted. • **reject**—Rejects the IPCP option if received from the peer. • **request**—Requests the DNS address from the peer.
header-compression ack	Enables IPCP header compression.
ignore-map	Ignores the dialer map when negotiating the peer IP address.
mask	Specifies IP address mask options: • *subnet-mask*—Specifies the subnet mask to offer the peer. • **reject**—Rejects subnet mask negotiations. • **request**—Requests the subnet mask from the peer.

username unique	Ignores a common username when providing an IP address to the peer.
wins	Specifies WINS options: • *primary-ip-address*—IP address of the primary WINS server. – *secondary-ip-address*—(Optional) IP address of the secondary WINS server. – .**aaa**—(Optional) Use WINS data from the AAA server. – **accept**—(Optional) Specifies that any nonzero WINS address will be accepted. • **accept**—Specifies that any nonzero WINS address will be accepted. • **reject**—Reject the IPCP option if received from the peer. • **request**—Request the WINS address from the peer.

Defaults

No servers are configured, and no address request is made.

Command Modes

Template configuration
Interface configuration (config-if)

Command History

Release	Modification
12.0(6)T	This command was introduced.
12.1(5)T	This command was modified. The **reject** and **accept** keywords were added.
Cisco IOS XE Release 3.2S	This command was modified. Support for IPv6 was added.

Examples

The following examples show use of the **ppp ipcp** command:

```
ppp ipcp accept-address

ppp ipcp dns 10.1.1.3

ppp ipcp dns 10.1.1.3 10.1.1.4

ppp ipcp dns 10.1.1.1 10.1.1.2 accept

ppp ipcp dns accept

ppp ipcp dns reject

ppp ipcp ignore-map

ppp ipcp username unique

ppp ipcp wins 10.1.1.1 10.1.1.2

ppp ipcp wins accept
```

The following examples show how to use the **no** form of the **ppp ipcp** command:

```
no ppp ipcp wins

no ppp ipcp ignore-map
```

Related Commands

Command	Description
debug ppp	Displays information on traffic and exchanges in an internetwork implementing the PPP.
show interfaces	Displays statistics for all interfaces configured on the router or access server.
show ip interfaces	Displays the usability status of interfaces configured for IP.

ppp multilink

To enable Multilink PPP (MLP) on an interface and, optionally, to enable Bandwidth Allocation Control Protocol (BACP) and its Bandwidth Allocation Protocol (BAP) subset for dynamic bandwidth allocation, use the **ppp multilink** command in interface configuration mode. To disable Multilink PPP or, optionally, to disable only dynamic bandwidth allocation, use the **no** form of this command.

ppp multilink [**bap**]

no ppp multilink [**bap** [**required**]]

Cisco 10000 Series Router

ppp multilink

no ppp multilink

Syntax Description

bap	(Optional) Specifies bandwidth allocation control negotiation and dynamic allocation of bandwidth on a link.
required	(Optional) Enforces mandatory negotiation of BACP for the multilink bundle. The multilink bundle is disconnected if BACP is not negotiated.

Defaults

This command is disabled. When BACP is enabled, the defaults are to accept calls and to set the timeout pending at 30 seconds.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.1	This command was introduced.
12.0(23)SX	This command was implemented on the Cisco 10000 series router.
12.2(16)BX	This command was implemented on the ESR–PRE2.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

This command applies only to interfaces that use PPP encapsulation.

MLP and PPP reliable links do not work together.

When the **ppp multilink** command is used, the first channel will negotiate the appropriate Network Control Protocol (NCP) layers (such as the IP Control Protocol and IPX Control Protocol), but subsequent links will negotiate only the link control protocol and MLP. NCP layers do not get negotiated on these links, and it is normal to see these layers in a closed state.

This command with the **bap** keyword must be used before configuring any **ppp bap** commands and options. If the **bap required** option is configured and a reject of the options is received, the multilink bundle is torn down.

The **no** form of this command without the **bap** keyword disables both MLP and BACP on the interface.

The **dialer load-threshold** command enables a rotary group to bring up additional links and to add them to a multilink bundle.

Before Cisco IOS Release 11.1, the **dialer-load threshold 1** command kept a multilink bundle of any number of links connected indefinitely, and the **dialer-load threshold 2** command kept a multilink bundle of two links connected indefinitely. If you want a multilink bundle to be connected indefinitely, you must set a very high idle timer.

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 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.

Cisco 10000 Series Router

The **ppp multilink** command has no arguments or keywords.

Examples

The following partial example shows how to configure a dialer for MLP:

```
interface Dialer0
 ip address 10.0.0.2 255.0.0.0
 encapsulation ppp
 dialer in-band
 dialer idle-timeout 500
 dialer map ip 10.0.0.1 name atlanta broadcast 81012345678901
 dialer load-threshold 30 either
 dialer-group 1
 ppp authentication chap
 ppp multilink
```

Related Commands

Command	Description
compress	Configures compression for LAPB, PPP, and HDLC encapsulations.
dialer fast-idle (interface)	Specifies the idle time before the line is disconnected.
dialer-group	Controls access by configuring an interface to belong to a specific dialing group.
dialer load-threshold	Configures bandwidth on demand by setting the maximum load before the dialer places another call to a destination.
encapsulation ppp	Enables PPP encapsulation.
ppp authentication	Enables CHAP or PAP or both, and specifies the order in which CHAP and PAP authentication is selected on the interface.
ppp bap timeout	Specifies nondefault timeout values for PPP BAP pending actions and responses.
ppp chap hostname	Enables a router calling a collection of routers that do not support this command to configure a common CHAP secret password to use in response to challenges from an unknown peer.

Command	Description
ppp multilink fragment delay	Specifies a maximum time for the transmission of a packet fragment on a MLP bundle.
ppp multilink fragment disable	Disables packet fragmentation.
ppp multilink fragmentation	Sets the maximum number of fragments a packet will be segmented into before being sent over the bundle.
ppp multilink group	Restricts a physical link to joining only a designated multilink-group interface.
ppp multilink interleave	Enables MLP interleaving.
ppp multilink mrru	Configures the MRRU value negotiated on an MLP bundle.
ppp multilink slippage	Defines the constraints that set the MLP reorder buffer size.
show ppp bap	Displays the configuration settings and run-time status for a multilink bundle.

ppp ncp override local

To track attributes received in authorization from RADIUS, verify the permitted Network Control Program (NCP), reject the current NCP negotiation, and override the local dual-stack configuration, use the **ppp ncp override local** command in global configuration mode. To disable the configuration, use the **no** form of this command.

ppp ncp override local

no ppp ncp override local

Syntax Description

This command has no arguments or keywords.

Command Default

The tracking of attributes from RADIUS and the local configuration override are not enabled. The local configuration is used.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines

Framed attributes are primarily used for address allocation. The RADIUS server maintains a pool of both IPv4 addresses and IPv6 prefixes. If IPv4 address or IPv6 prefix attributes are absent in the access-accept response from RADIUS, the **ppp ncp override local** command can be used to override local configuration.

Examples

The following example shows how to override the local IPv6 or IPv4 dual-stack configuration:

```
Router> enable
Router# configure terminal
Router(config)# ppp ncp override local
```

ppp timeout ncp

To set a time limit for the successful negotiation of at least one network layer protocol after a PPP connection is established, use the **ppp timeout ncp** command in interface configuration mode. To remove the time limit, use the **no** form of this command.

ppp timeout ncp *seconds*

no ppp timeout ncp

Syntax Description

seconds	Maximum time, in seconds, PPP should wait for negotiation of a network layer protocol. If no network protocol is negotiated in the given time, the connection is disconnected.

Defaults

No time limit is imposed.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.3	This command was introduced as **ppp negotiation-timeout**.
12.2	This command was changed to **ppp timeout ncp**. The **ppp negotiation-timeout** command was accepted by the command line interpreter through Cisco IOS Release 12.2.
Cisco IOS XE Release 3.2S	Support for IPv6 was added.

Usage Guidelines

The **ppp timeout ncp** command protects against the establishment of links that are physically up and carrying traffic at the link level, but are unusable for carrying data traffic due to failure to negotiate the capability to transport any network level data. This command is particularly useful for dialed connections, where it is usually undesirable to leave a telephone circuit active when it cannot carry network traffic.

Examples

The following example sets the Network Control Protocol (NCP) timer to 8 seconds:

```
ppp timeout ncp 8
```

Related Commands

Command	Description
absolute-timeout	Sets the interval for closing user connections on a specific line or port.
dialer idle-timeout (interface)	Specifies the idle time before the line is disconnected.

ppp unique address accept-access

To track duplicate addresses received from RADIUS and create a standalone database, use the **ppp unique address accept-access** command in global configuration mode. To disable this feature and remove the database, use the **no** form of this command.

ppp unique address accept-access

no ppp unique address accept-access

Syntax Description

This command has no arguments or keywords.

Command Default

This feature is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines

The **ppp unique address accept-access** command enables the IPv6 router to track and check duplicate attributes received in an Access-Accept response from RADIUS, and triggers creation of a new, standalone database that contains the Access-Accept responses received since the feature was enabled.

The following RADIUS attributes are tracked in this database and checked when an Access-Accept response is received:

- Framed-IP-Address
- Framed-IPv6-Prefix
- Delegated-IPv6-Prefix

All of these RADIUS attributes from this list are checked against the database for duplicates and, if none are found, added to the database exactly as presented in the RADIUS attribute.

Examples

The following example enables this feature:

```
Router (config)# ppp unique address accept-access
```

prc-interval (IPv6)

To configure the hold-down period between partial route calculations (PRCs), use the **prc-interval** command in address family configuration mode. To restore the default interval, use the **no** form of this command.

prc-interval *seconds* [*initial-wait*] [*secondary-wait*]

no prc-interval *seconds*

Syntax Description

seconds	Minimum amount of time between PRCs, in seconds. It can be a number in the range 1 to 120. The default is 5 seconds.
initial-wait	(Optional) Length of time before the first PRC in milliseconds.
secondary-wait	(Optional) Minimum length of time between the first and second PRC in milliseconds.

Command Default

The default is 5 seconds.

Command Modes

Address family configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
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.
12.2(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 2.6	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The **prc-interval** command is used only in multitopology Intermediate System-to-Intermediate System (IS-IS).

The **prc-interval** command controls how often Cisco IOS software can perform a PRC. Increasing the PRC interval reduces the processor load of the router, but it could slow the convergence.

This command is analogous to the **spf-interval** command, which controls the hold-down period between shortest path first (SPF) calculations.

You can use the **prc-interval** (IPv6) command only when using the IS-IS multitopology for IPv6 feature.

Examples

The following example sets the PRC calculation interval to 20 seconds:

```
Router(config)# router isis
Router(config-router)# address-family ipv6
Router(config-router-af)# prc-interval 20
```

Related Commands

Command	Description
spf-interval (IPv6)	Controls how often Cisco IOS software performs the SPF calculation.

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.

prefix-delegation

To specify a manually configured numeric prefix to be delegated to a specified client (and optionally a specified identity association for prefix delegation [IAPD] for that client), use the **prefix-delegation** command in DHCP for IPv6 pool configuration mode. To remove the prefix, use the **no** form of this command.

prefix-delegation *ipv6-prefix/prefix-length client-DUID* [**iaid** *iaid*] [*lifetime*]

no prefix-delegation *ipv6-prefix/prefix-length client-DUID* [**iaid** *iaid*]

Syntax Description

ipv6-prefix	(Optional) Specified IPv6 prefix. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/prefix-length	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address).
client-DUID	The DHCP unique identifier (DUID) of the client to which the prefix is delegated.
iaid *iaid*	(Optional) Identity association identifier (IAID), which uniquely identifies an IAPD on the client.
lifetime	(Optional) Sets a length of time over which the requesting router is allowed to use the prefix. The following values can be used: • **valid-lifetime**—The length of time, in seconds, that the prefix remains valid for the requesting router to use. • **at**—Specifies absolute points in time where the prefix is no longer valid and no longer preferred. • **infinite**—Indicates an unlimited lifetime. • **preferred-lifetime**—The length of time, in seconds, that the prefix remains preferred for the requesting router to use. • *valid-month valid-date valid-year valid-time*—A fixed duration of time for hosts to remember router advertisements. The format to be used can be **oct 24 2003 11:45** or **24 oct 2003 11:45**. • *preferred-month preferred-date preferred-year preferred-time*—A fixed duration of time for hosts to remember router advertisements. The format to be used can be **oct 24 2003 11:45** or **24 oct 2003 11:45**.

Command Default

No manually configured prefix delegations exist.

Command Modes

DHCP for IPv6 pool configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

Administrators can manually configure a list of prefixes and associated preferred and valid lifetimes for an IAPD of a specific client that is identified by its DUID. This static binding of client and prefixes can be specified based on users' subscription to an ISP using the **prefix-delegation** *prefix-length* command.

The *client-DUID* argument identifies the client to which the prefix is delegated. All the configured prefixes will be assigned to the specified IAPD of the client. The IAPD to which the prefix is assigned is identified by the **iaid** argument if the **iaid** keyword is configured. If the **iaid** keyword is not configured, the prefix will be assigned to the first IAPD from the client that does not have a static binding. This function is intended to make it convenient for administrators to manually configure prefixes for a client that only sends one IAPD in case it is not easy to know the iaid in advance.

When the delegating router receives a request from a client, it checks whether there is a static binding configured for the IAPD in the client's message. If one is present, the prefixes in the binding are returned to the client. If no such binding is found, the server attempts to assign prefixes for the client from other sources.

Optionally valid and preferred lifetimes can be specified for the prefixes assigned from this pool. Users should coordinate the specified lifetimes with the lifetimes on prefixes from the upstream delegating router if the prefixes were acquired from that router.

The **lifetime** keyword can be specified in one of two ways:

- A fixed duration that stays the same in consecutive advertisements.
- Absolute expiration time in the future so that advertised lifetime decrements in real time, which will result in a lifetime of 0 at the specified time in the future.

The specified length of time is between 60 and 4294967295 seconds or infinity if the **infinite** keyword is specified.

Examples

The following example configures an IAPD for a specified client:

```
prefix-delegation 2001:0DB8::/64 00030001000BBFAA2408
```

Related Commands

Command	Description
ipv6 dhcp pool	Configures a DHCP for IPv6 pool and enters DHCP for IPv6 pool configuration mode.
ipv6 local pool	Configures a local IPv6 prefix pool.
prefix-delegation pool	Specifies a named IPv6 local prefix pool from which prefixes are delegated to DHCP for IPv6 clients.
show ipv6 dhcp pool	Displays DHCP for IPv6 configuration pool information.

prefix-delegation aaa

To specify that prefixes are to be acquired from authorization, authentication, and accounting (AAA) servers, use the **prefix-delegation aaa** command in DHCP for IPv6 pool configuration mode. To disable this feature, use the **no** form of this command.

Cisco IOS Release 12.4(22)T and Earlier Releases and Cisco IOS Release 12.2(18)SXE, Cisco IOS XE Release 2.1, and Later Releases

prefix-delegation aaa [**method-list** *method-list* [**lifetime**] {{*valid-lifetime* | **infinite**} {*valid-lifetime* | **infinite**} | **at** {*date month year time* | *month date year time*} {*date month year time* | *month date year time*}}]

no prefix-delegation aaa method-list *method-list*

Cisco IOS Release 15.0(1)M and Later Releases

prefix-delegation aaa method-list {*method-list* | **default**} [**lifetime** {*valid-lifetime* | **infinite**} {*preferred-lifetime* | **infinite**} | **at** {*date month year time* | *month date year time*} {*date month year time* | *month date year time*}]

no prefix-delegation aaa method-list *method-list*

Syntax Description

method-list	(Optional) Indicates a method list to be defined.
method-list	Configuration type AAA authorization method list that defines how authorization will be performed.
default	Specifies the default method list, nvgened.
lifetime	(Optional) Configures prefix lifetimes.
valid-lifetime	The length of time that the prefix remains valid for the requesting router to use, in seconds. The range is from 60 to 4294967295. The default value is 2592000 seconds.
infinite	Indicates an unlimited lifetime.
preferred-lifetime	The length of time that the prefix remains preferred for the requesting router to use, in seconds. The range is from 60 to 4294967295. The default value is 604800 seconds.
at	Specifies absolute points in time where the prefix is no longer valid and no longer preferred.
date	The date for the valid lifetime to expire.
month	The month for the valid lifetime to expire.
year	The year for the valid lifetime to expire. The range is from 2003 to 2035.
time	The year for the valid lifetime to expire.

Command Default

The default time that the prefix remains valid is 2592000 seconds, and the default time that the prefix remains preferred for the requesting router to use is 604800 seconds.

Command Modes DHCP for IPv6 pool configuration (config-dhcpv6)

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.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.0(1)M	This command was modified. The **default** keyword was added and the command syntax was modified to show that **lifetime** can be configured only to a **method-list**.
Cisco IOS XE Release 2.5	This command was updated. It was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines In order for the Dynamic Host Configuration Protocol (DHCP) for IPv6 server to obtain prefixes from RADIUS servers, you must also configure the AAA client and Point-to-Point Protocol (PPP) on the router. For information on how to configure the AAA client and PPP, see the "Implementing ADSL and Deploying Dial Access for IPv6" module.

Use the **aaa authorization configuration default**, **aaa group server radius**, and **radius-server host** commands to specify a named list of authorization method and RADIUS servers to contact to acquire prefixes, and then apply that named list to the **prefix-delegation aaa** command.

Valid and preferred lifetimes can be specified for the prefixes assigned from AAA servers.

The **prefix-delegation aaa** and **prefix-delegation pool** commands are mutually exclusive in a pool.

Examples The following example shows how to specify the use of a method list named list1:

```
Router> enable
Router# configure terminal
Router(config)# ipv6 dhcp pool name
Router(config-dhcpv6)# prefix-delegation aaa method-list list1
```

Related Commands

Command	Description
aaa authorization configuration default	Downloads static route configuration information from the AAA server using TACACS+ or RADIUS.
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
prefix-delegation pool	Specifies a named IPv6 local prefix pool from which prefixes are delegated to DHCP for IPv6 clients.
radius-server host	Specifies a RADIUS server host.
sip address	Configures a SIP server IPv6 address to be returned in the SIP server's IPv6 address list option to clients.
sip domain-name	Configures an SIP server domain name to be returned in the SIP server's domain name list option to clients.

prefix-delegation pool

To specify a named IPv6 local prefix pool from which prefixes are delegated to Dynamic Host Configuration Protocol (DHCP) for IPv6 clients, use the **prefix-delegation pool** command in DHCP for IPv6 pool configuration mode. To remove a named IPv6 local prefix pool, use the **no** form of this command.

prefix-delegation pool *poolname* [**lifetime** {*valid-lifetime preferred-lifetime*}]

no prefix-delegation pool *poolname*

Syntax Description

poolname	User-defined name for the local prefix pool. The pool name can be a symbolic string (such as "Engineering") or an integer (such as 0).
lifetime	(Optional) Used to set a length of time for the hosts to remember router advertisements. If the optional **lifetime** keyword is configured, both valid and preferred lifetimes must be configured.
valid-lifetime	The amount of time that the prefix remains valid for the requesting router to use. The following values can be used: • *seconds*—The length of time, in seconds, that the prefix remains valid for the requesting router to use. The range is from 60 through 4294967295. The *preferred-lifetime* value cannot exceed the *valid-lifetime* value. • **at**—Specifies absolute points in time where the prefix is no longer valid and no longer preferred. • **infinite**—Indicates an unlimited lifetime. • *valid-month valid-date valid-year valid-time*—A fixed duration of time for hosts to remember router advertisements. The format to be used can be **oct 24 2003 11:45** or **24 oct 2003 11:45**.
preferred-lifetime	The length of time, in seconds, that the prefix remains preferred for the requesting router to use. The following values can be used: • *seconds*—The length of time, in seconds, that the prefix remains valid for the requesting router to use. The range is from 60 through 4294967295. The *preferred-lifetime* value cannot exceed the *valid-lifetime* value. • **at**—Specifies absolute points in time where the prefix is no longer valid and no longer preferred. • **infinite**—Indicates an unlimited lifetime. • *preferred-month preferred-date preferred-year preferred-time*—A fixed duration of time for hosts to remember router advertisements. The format to be used can be **oct 24 2003 11:45** or **24 oct 2003 11:45**

Command Default

No IPv6 local prefix pool is specified.
Valid lifetime is 2592000 seconds (30 days).
Preferred lifetime is 604800 seconds (7 days).

Command Modes

DHCP for IPv6 pool configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

The **prefix-delegation pool** command specifies a named IPv6 local prefix pool from which prefixes are delegated to clients. Use the **ipv6 local pool** command to configure the named IPv6 prefix pool.

Optionally, valid and preferred lifetimes can be specified for the prefixes assigned from this pool. Users should coordinate the specified lifetimes with the lifetimes on prefixes from the upstream delegating router if the prefixes were acquired from that router.

The **lifetime** keyword can be specified in one of two ways:

- A fixed duration that stays the same in consecutive advertisements.
- Absolute expiration time in the future so that advertised lifetime decrements in real time, which will result in a lifetime of 0 at the specified time in the future.

The specified length of time is from 60 to 4,294,967,295 seconds or infinity if the **infinite** keyword is specified.

The Cisco IOS DHCP for IPv6 server can assign prefixes dynamically from an IPv6 local prefix pool, which is configured using the **ipv6 local pool** command and associated with a DHCP for IPv6 configuration pool using the **prefix-delegation pool** command. When the server receives a prefix request from a client, it attempts to obtain unassigned prefixes, if any, from the pool.

After the client releases the previously assigned prefixes, the server will return the prefixes to the pool for reassignment to other clients.

Examples

The following example specifies that prefix requests should be satisfied from the pool called client-prefix-pool. The prefixes should be delegated with the valid lifetime set to 1800 seconds, and the preferred lifetime is set to 600 seconds:

```
prefix-delegation pool client-prefix-pool lifetime 1800 600
```

Related Commands

Command	Description
ipv6 dhcp pool	Configures a DHCP for IPv6 pool and enters DHCP for IPv6 pool configuration mode.
ipv6 local pool	Configures a local IPv6 prefix pool.
prefix-delegation	Specifies a manually configured numeric prefix that is to be delegated to a particular client's IAPD.
show ipv6 dhcp pool	Displays DHCP for IPv6 configuration pool information.

process-min-time percent

Note Effective with Cisco IOS 15.1(1)T release, the **process-min-time percent** command is not available in Cisco IOS 15.1(1)T and later releases. Improvements in Cisco IOS scheduler have made this command unnecessary.

To specify the minimum percentage of CPU process time OSPF takes before the CPU should yield to a process with a higher priority, use the **process-min-time percent** command in router configuration mode. To disable this function, use the **no** form of this command.

process-min-time percent *percentage*

no process-min-time percent

Syntax Description

percentage	Percentage of CPU process time to be used before trying to release the CPU for other processes. The valid value range is from 1 to 100. The default is 25.

Command Default

The default is 25 percent.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
12.2(18)SXF	This command was introduced on the Supervisor Engine 720 and the Supervisor Engine 320.
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.
15.1(1)T	This command was removed.

Usage Guidelines

Note Use this command under the direction of Cisco TAC only.

This command is supported by OSPFv2 and OSPFv3.

Use the **process-min-time percent** command to configure the minimum percentage of the process maximum time. Lowering the minimum percentage of CPU usage that a process can utilize is useful in some circumstances to ensure equitable division of CPU resources among different tasks. Once the percentage has been exceeded, CPU control may be given to a higher priority process.

The process maximum time is set using the **process-max-time** command. Use the **process-min-time percent** command in conjunction with the **process-max-time** command.

Examples

The following example shows how to set the percentage of CPU process time to be used before releasing the CPU:

```
Router# configure terminal
Router(config)# router ospf
Router(config-router)# process-min-time percent 35
```

The following example shows how to return to the default setting in IPv4:

```
Router# configure terminal
Router(config)# router ospf
Router(config-router)# no process-min-time percent
```

Related Commands

Command	Description
process-max-time	Configures the amount of time after which a process should voluntarily yield to another process.

protocol ipv6 (ATM)

To map the IPv6 address of a remote node to the ATM permanent virtual circuit (PVC) used to reach the address, use the **protocol ipv6** command in ATM VC configuration mode. To remove the static map, use the **no** form of this command.

protocol ipv6 *ipv6-address* [[**no**] **broadcast**]

no protocol ipv6 *ipv6-address* [[**no**] **broadcast**]

Syntax Description

ipv6-address	Destination IPv6 (protocol) address that is being mapped to a PVC. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
no broadcast	(Optional) Indicates whether the map entry should be used when IPv6 multicast packets (not broadcast packets) are sent to the interface. Pseudobroadcasting is supported. The [**no**] **broadcast** keywords in the **protocol ipv6** command take precedence over the **broadcast** command configured on the same ATM PVC.

Command Default

No mapping is defined.

Command Modes

ATM VC configuration (for an ATM PVC)

Command History

Release	Modification
12.2(2)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 Release 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.

Examples

In the following example, two nodes named Cisco 1 and Cisco 2 are connected by a single PVC. The point-to-point subinterface ATM0.132 is used on both nodes to terminate the PVC; therefore, the mapping between the IPv6 addresses of both nodes and the PVC is implicit (no additional mappings are required).

Cisco 1 Configuration

```
interface ATM0
 no ip address
!
interface ATM0.132 point-to-point
 pvc 1/32
```

```
  encapsulation aal5snap
 !
 ipv6 address 2001:0DB8:2222::72/32
```

Cisco 2 Configuration

```
interface ATM0
 no ip address
!
interface ATM0.132 point-to-point
 pvc 1/32
  encapsulation aal5snap
 !
 ipv6 address 2001:0DB8:2222::45/32
```

In the following example, the same two nodes (Cisco 1 and Cisco 2) from the previous example are connected by the same PVC. In this example, however, the point-to-multipoint interface ATM0 is used on both nodes to terminate the PVC; therefore, explicit mappings are required between the link-local and global IPv6 addresses of interface ATM0 on both nodes and the PVC. Additionally, ATM pseudobroadcasts are enabled on the link-local address of interface ATM0 on both nodes.

Cisco 1 Configuration

```
interface ATM0
 no ip address
 pvc 1/32
  protocol ipv6 2001:0DB8:2222::45
  protocol ipv6 FE80::60:2FA4:8291:2 broadcast
  encapsulation aal5snap
 !
 ipv6 address 2001:0DB8:2222::72/32
```

Cisco 2 Configuration

```
interface ATM0
 no ip address
 pvc 1/32
  protocol ipv6 FE80::60:3E47:AC8:C broadcast
  protocol ipv6 2001:0DB8:2222::72
  encapsulation aal5snap
 !
 ipv6 address 2001:0DB8:2222::45/32
```

Related Commands

Command	Description
show atm map	Displays the list of all configured ATM static maps to remote hosts on an ATM network and on ATM bundle maps.

protocol mode

To configure the Cisco IOS Session Initiation Protocol (SIP) stack, use the **protocol mode** command in SIP user-agent configuration mode. To disable the configuration, use the **no** form of this command.

protocol mode {**ipv4** | **ipv6** | **dual-stack** [**preference** {**ipv4** | **ipv6**}]}

no protocol mode

Syntax Description

ipv4	Specifies the IPv4-only mode.
ipv6	Specifies the IPv6-only mode.
dual-stack	Specifies the dual-stack (that is, IPv4 and IPv6) mode.
preference {**ipv4** | **ipv6**}	(Optional) Specifies the preferred dual-stack mode, which can be either IPv4 (the default preferred dual-stack mode) or IPv6.

Command Default

No protocol mode is configured.
The Cisco IOS SIP stack operates in IPv4 mode when the **no protocol mode** or **protocol mode ipv4** command is configured.

Command Modes

SIP user-agent configuration (config-sip-ua)

Command History

Release	Modification
12.4(22)T	This command was introduced.
15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.

Usage Guidelines

The **protocol mode** command is used to configure the Cisco IOS SIP stack in IPv4-only, IPv6-only, or dual-stack mode. For dual-stack mode, the user can (optionally) configure the preferred family, IPv4 or IPv6.

For a particular mode (for example, IPv6-only), the user can configure any address (for example, both IPv4 and IPv6 addresses) and the system will not hide or restrict any commands on the router. SIP chooses the right address for communication based on the configured mode on a per-call basis.

For example, if the domain name system (DNS) reply has both IPv4 and IPv6 addresses and the configured mode is IPv6-only (or IPv4-only), the system discards all IPv4 (or IPv6) addresses and tries the IPv6 (or IPv4) addresses in the order they were received in the DNS reply. If the configured mode is dual-stack, the system first tries the addresses of the preferred family in the order they were received in the DNS reply. If all of the addresses fail, the system tries addresses of the other family.

Examples

The following example configures dual-stack as the protocol mode:

```
Router(config-sip-ua)# protocol mode dual-stack
```

The following example configures IPv6 only as the protocol mode:

```
Router(config-sip-ua)# protocol mode ipv6
```

The following example configures IPv4 only as the protocol mode:

```
Router(config-sip-ua)# protocol mode ipv4
```

The following example configures no protocol mode:

```
Router(config-sip-ua)# no protocol mode
```

Related Commands

Command	Description
sip ua	Enters SIP user-agent configuration mode.

queue-depth (OSPFv3)

To configure the number of incoming packets that the IPv4 Open Shortest Path First version 3 (OSPFv3) process can keep in its queue, use the **queue-depth** command in OSPFv3 router configuration mode. To set the queue depth to its default value, use the **no** form of the command.

queue-depth {**hello** | **update**} {*queue-size* | **unlimited**}

no queue-depth {**hello** | **update**}

Syntax Description

hello	Specifies the queue depth of the OSPFv3 hello process.
update	Specifies the queue depth of the OSPFv3 router process queue.
queue-size	Maximum number of packets in the queue. The range is 1 to 2147483647.
unlimited	Specifies an infinite queue depth.

Command Default

If you do not set a queue size, the OSPFv3 hello process queue depth is unlimited and the OSPFv3 router process (update) queue depth is 200 packets.

Command Modes

OSPFv3 router configuration mode (config-router)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

All incoming OSPFv3 packets are initially enqueued in the hello queue. OSPFv3 hello packets are processed directly from this queue, while all other OSPFv3 packet types are subsequently enqueued in the update queue.

If you configure a router with many neighbors and a large database, use the **queue-depth** command to adjust the size of the hello and router queues. Otherwise, packets might be dropped because of queue limits, and OSPFv3 adjacencies may be lost.

Examples

The following example shows how to configure the OSPFv3 update queue to 1500 packets:

```
Router(config)# router ospfv3 1
Router(config-router)# queue-depth update 1500
```

Related Commands

Command	Description
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

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 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 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 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 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.

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.

redistribute (IPv6)

To redistribute IPv6 routes from one routing domain into another routing domain, use the **redistribute** command in address family configuration or router configuration mode. To disable redistribution, use the **no** form of this command.

redistribute *source-protocol* [*process-id*] [**include-connected** {**level-1** | **level-1-2** | **level-2**}] [*as-number*] [**metric** {*metric-value* | **transparent**}] [**metric-type** *type-value*] [**match** {**external** [**1** | **2**] | **internal** | **nssa-external** [**1** | **2**]}] [**tag** *tag-value*] [**route-map** *map-tag*]

no redistribute *source-protocol* [*process-id*] [**include-connected**] {**level-1** | **level-1-2** | **level-2**} [*as-number*] [**metric** {*metric-value* | **transparent**}] [**metric-type** *type-value*] [**match** {**external** [**1** | **2**] | **internal** | **nssa-external** [**1** | **2**]}] [**tag** *tag-value*] [**route-map** *map-tag*]

Syntax Description

source-protocol	Source protocol from which routes are being redistributed. It can be one of the following keywords: **bgp**, **connected**, **eigrp**, **isis**, **ospf**, **rip**, or **static**.
process-id	(Optional) For the **bgp** or **eigrp** keyword, the process ID is a Border Gateway Protocol (BGP) autonomous system number, which is a 16-bit decimal number. For the **isis** keyword, the process ID is an optional value that defines a meaningful name for a routing process. You can specify only one IS-IS process per router. Creating a name for a routing process means that you use names when configuring routing. For the **ospf** keyword, the process ID is the number assigned administratively when the Open Shortest Path First (OSPF) for IPv6 routing process is enabled. For the **rip** keyword, the process ID is an optional value that defines a meaningful name for an IPv6 Routing Information Protocol (RIP) routing process.
include-connected	(Optional) Allows the target protocol to redistribute routes learned by the source protocol and connected prefixes on those interfaces over which the source protocol is running.
level-1	Specifies that, for Intermediate System-to-Intermediate System (IS-IS), Level 1 routes are redistributed into other IP routing protocols independently.
level-1-2	Specifies that, for IS-IS, both Level 1 and Level 2 routes are redistributed into other IP routing protocols.
level-2	Specifies that, for IS-IS, Level 2 routes are redistributed into other IP routing protocols independently.
as-number	(Optional) Autonomous system number for the redistributed route.
metric *metric-value*	(Optional) When redistributing from one OSPF process to another OSPF process on the same router, the metric will be carried through from one process to the other if no metric value is specified. When redistributing other processes to an OSPF process, the default metric is 20 when no metric value is specified.
metric transparent	(Optional) Causes RIP to use the routing table metric for redistributed routes as the RIP metric.

metric-type *type-value*	(Optional) For OSPF, specifies the external link type associated with the default route advertised into the OSPF routing domain. It can be one of two values: • **1**—Type 1 external route • **2**—Type 2 external route If no value is specified for the **metric-type** keyword, the Cisco IOS software adopts a Type 2 external route. For IS-IS, the link type can be one of two values: • **internal**—IS-IS metric that is < 63. • **external**—IS-IS metric that is > 64 < 128. The default is **internal**.
match {**external [1 | 2] | internal | nssa-external [1 | 2]**}	(Optional) For OSPF, routes are redistributed into other routing domains using the **match** keyword. It is used with one of the following: • **external [1 | 2]**—Routes that are external to the autonomous system, but are imported into OSPF as Type 1 or Type 2 external routes. • **internal**—Routes that are internal to a specific autonomous system. • **nssa-external** [**1 | 2**]—Routes that are external to the autonomous system but are imported into OSPF, in a not so stubby area (NSSA), for IPv6 as Type 1 or Type 2 external routes.
tag *tag-value*	(Optional) Specifies the 32-bit decimal value attached to each external route. This is not used by OSPF itself. It may be used to communicate information between Autonomous System Boundary Routers (ASBRs). If none is specified, then the remote autonomous system number is used for routes from BGP and Exterior Gateway Protocol (EGP); for other protocols, zero (0) is used.
route-map	(Optional) Specifies the route map that should be checked to filter the importation of routes from this source routing protocol to the current routing protocol. If the **route-map** keyword is not specified, all routes are redistributed. If this keyword is specified, but no route map tags are listed, no routes will be imported.
map-tag	(Optional) Identifier of a configured route map.

Command Default

Route redistribution is disabled.

Command Modes

Address family configuration
Router configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.4(6)T	Support for Enhanced Internal Gateway Routing Protocol (EIGRP) IPv6 was 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.
12.2(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 introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

Changing or disabling any keyword will not affect the state of other keywords.

A router receiving an IPv6 IS-IS route with an internal metric will consider the cost of the route from itself to the redistributing router plus the advertised cost to reach the destination. An external metric considers only the advertised metric to reach the destination.

IS-IS will ignore any configured redistribution of routes configured with the **include-connected** keyword. IS-IS will advertise a prefix on an interface if either IS-IS is running over the interface or the interface is configured as passive.

Routes learned from IPv6 routing protocols can be redistributed into IPv6 IS-IS at Level 1 into an attached area or at Level 2. The **level-1-2** keyword allows both Level 1 and Level 2 routes in a single command.

For IPv6 RIP, use the **redistribute** command to advertise static routes as if they were directly connected routes.

Caution Advertising static routes as directly connected routes can cause routing loops if improperly configured.

Redistributed IPv6 RIP routing information should always be filtered by the **distribute-list prefix-list** router configuration command. Use of the **distribute-list prefix-list** command ensures that only those routes intended by the administrator are passed along to the receiving routing protocol.

Note The **metric** value specified in the **redistribute** command for IPv6 RIP supersedes the **metric** value specified using the **default-metric** command.

Note In IPv4, if you redistribute a protocol, by default you also redistribute the subnet on the interfaces over which the protocol is running. In IPv6 this is not the default behavior. To redistribute the subnet on the interfaces over which the protocol is running in IPv6, use the **include-connected** keyword. In IPv6 this functionality is not supported when the source protocol is BGP.

When the **no redistribute** command is configured, the parameter settings are ignored when the client protocol is IS-IS or EIGRP.

IS-IS redistribution will be removed completely when IS-IS level 1 and level 2 are removed by the user. IS-IS level settings can be configured using the **redistribute** command only.

The default redistribute type will be restored to OSPF when all route type values are removed by the user.

Examples

The following example configures IPv6 IS-IS to redistribute IPv6 BGP routes. The metric is specified as 5, and the metric type will be set to external, indicating that it has lower priority than internal metrics.

```
Router(config)# router isis
Router(config-router)# address-family ipv6
Router(config-router-af)# redistribute bgp 64500 metric 5 metric-type external
```

The following example redistributes IPv6 BGP routes into the IPv6 RIP routing process named cisco:

```
Router(config)# ipv6 router rip cisco
Router(config-router)# redistribute bgp 42
```

The following example redistributes IS-IS for IPv6 routes into the OSPF for IPv6 routing process 1:

```
Router(config)# ipv6 router ospf 1
Router(config-router)# redistribute isis 1 metric 32 metric-type 1 tag 85
```

In the following example, ospf 1 redistributes the prefixes 2001:1:1::/64 and 2001:99:1::/64 and any prefixes learned through rip 1:

```
interface ethernet0/0
 ipv6 address 2001:1:1::90/64
 ipv6 rip 1 enable

interface ethernet1/1
 ipv6 address 2001:99:1::90/64
 ipv6 rip 1 enable

interface ethernet2/0
 ipv6 address 2001:1:2::90/64
 ipv6 ospf 1 area 1

ipv6 router ospf 1
  redistribute rip 1 include-connected
```

The following configuration example and output show the **no redistribute** command parameters when the last route type value is removed:

```
Router(config-router)# redistribute rip process1 metric 7
Router(config-router)# do show run | include redistribute
 redistribute rip process1 metric 7
Router(config-router)# no redistribute rip process1 metric 7
Router(config-router)# do show run | include redistribute
 redistribute rip process1
Router(config-router)#
```

Related Commands

Command	Description
default-metric	Specifies a default metric for redistributed routes.
distribute-list prefix-list (IPv6 EIGRP)	Applies a prefix list to EIGRP for IPv6 routing updates that are received or sent on an interface.
distribute-list prefix-list (IPv6 RIP)	Applies a prefix list to IPv6 RIP routing updates that are received or sent on an interface.
redistribute isis (IPv6)	Redistributes IPv6 routes from one routing domain into another routing domain using IS-IS as both the target and source protocol.

redistribute (OSPFv3)

To redistribute IPv6 and IPv4 routes from one routing domain into another routing domain, use the **redistribute** command in IPv6 or IPv4 address family configuration mode. To disable redistribution, use the **no** form of this command.

redistribute *source-protocol* [*process-id*] [*options*]

no redistribute *source-protocol* [*process-id*] [*options*]

Syntax Description

source-protocol	Source protocol from which routes are being redistributed. It can be one of the following keywords: **bgp**, **connected**, **eigrp**, **isis**, **nd**, **nemo**, **ospfv3**, **ospf**, **rip**, or **static**.
process-id	(Optional) For the **bgp** or **eigrp** keyword, the process ID is a Border Gateway Protocol (BGP) autonomous system number, which is a 16-bit decimal number. For the **isis** keyword, the process ID is an optional value that defines a meaningful name for a routing process. You can specify only one IS-IS process per router. Creating a name for a routing process means that you use names when configuring routing. For the **ospfv3** keyword, the process ID is the number assigned administratively when the Open Shortest Path First version 3 (OSPFv3) routing process is enabled. For the **rip** keyword, the process ID is an optional value that defines a meaningful name for an IPv6 Routing Information Protocol (RIP) routing process.
options	(Optional)

Command Default

Default redistribute type is OSPFv3.

Command Modes

IPv6 address family configuration (config-router-af)
IPv4 address family configuration (config-router-af)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

Changing or disabling any keyword will not affect the state of other keywords.

For the IPv6 address family (AF), the **ospf** option refers to an OSPFv3 process. For the IPv4 address family, the **ospfv3** option specifies an OSPFv3 process, and the **ospf** option refers to an OSPFv2 process.

A router receiving an IPv6 IS-IS route with an internal metric will consider the cost of the route from itself to the redistributing router plus the advertised cost to reach the destination. An external metric considers only the advertised metric to reach the destination.

IS-IS will ignore any configured redistribution of routes configured with the **include-connected** keyword. IS-IS will advertise a prefix on an interface if either IS-IS is running over the interface or the interface is configured as passive.

Routes learned from IPv6 routing protocols can be redistributed into IPv6 IS-IS at Level 1 into an attached area or at Level 2. The **level-1-2** keyword allows both Level 1 and Level 2 routes in a single command.

For IPv6 RIP, use the **redistribute** command to advertise static routes as if they were directly connected routes.

Caution Advertising static routes as directly connected routes can cause routing loops if improperly configured.

Redistributed IPv6 RIP routing information should always be filtered by the **distribute-list prefix-list** router configuration command. Use of the **distribute-list prefix-list** command ensures that only those routes intended by the administrator are passed along to the receiving routing protocol.

Note The **metric** value specified in the **redistribute** command for IPv6 RIP supersedes the **metric** value specified using the **default-metric** command.

Note In IPv4, if you redistribute a protocol, by default you also redistribute the subnet on the interfaces over which the protocol is running. In IPv6, this is not the default behavior. To redistribute the subnet on the interfaces over which the protocol is running in IPv6, use the **include-connected** keyword. In IPv6, this functionality is not supported when the source protocol is BGP.

When the **no redistribute** command is configured, the parameter settings are ignored when the client protocol is IS-IS or EIGRP.

IS-IS redistribution will be removed completely when IS-IS level 1 and level 2 are removed by the user. IS-IS level settings can be configured using the **redistribute** command only.

The default redistribute type will be restored to OSPFv3 when all route type values are removed by the user.

Examples

The following example :

Related Commands

Command	Description
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

redistribute isis (IPv6)

To redistribute IPv6 routes from one routing domain into another routing domain using Intermediate System-to-Intermediate System (IS-IS) as both the target and source protocol, use the **redistribute isis** command in address family configuration. To disable redistribution, use the **no** form of this command.

redistribute isis [*process-id*] {**level-1** | **level-2**} **into** {**level-1** | **level-2**} **distribute-list** *list-name*

no redistribute isis [*process-id*] {**level-1** | **level-2**} **into** {**level-1** | **level-2**} **distribute-list** *list-name*

Syntax Description

process-id	(Optional) An optional *tag* value that defines a meaningful name for a routing process. You can specify only one IS-IS process per router. Creating a name for a routing process means that you use names when configuring routing.
level-1	Specifies that IS-IS Level 1 routes are redistributed into other IP routing protocols independently.
level-2	Specifies that IS-IS Level 2 routes are redistributed into other IP routing protocols independently.
into	Distributes IS-IS Level 1 or Level 2 routes into Level 1 or Level 2 in another IS-IS instance.
distribute-list	Distribute list used for the redistributed route.
list-name	Name of the distribute list for the redistributed route.

Command Default

Route redistribution is disabled.
process-id: No process ID is defined.

Command Modes

Address family configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
Cisco IOS XE Release 2.4	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

Changing or disabling any keyword will not affect the state of other keywords.

A router receiving an IPv6 IS-IS route with an internal metric will consider the cost of the route from itself to the redistributing router plus the advertised cost to reach the destination. An external metric only considers the advertised metric to reach the destination.

IS-IS will ignore any configured redistribution of routes configured with the **connected** keyword. IS-IS will advertise a prefix on an interface if either IS-IS is running over the interface or the interface is configured as passive.

Routes learned from IPv6 routing protocols can be redistributed into IPv6 IS-IS at Level 1 into an attached area or at Level 2. The **level-1-2** keyword allows both Level 1 and Level 2 routes in a single command.

Examples

The following examples shows how to redistribute IPv6 routes from level 1 to level 2:

```
redistribute isis level-1 into level-2
```

Related Commands

Command	Description
default-metric	Specifies a default metric for redistributed routes.
redistribute (IPv6)	Redistributes IPv6 routes from one routing domain into another routing domain.

register (mobile router)

To control the registration parameters of the IPv6 mobile router, use the **register** command in mobile router configuration mode or IPv6 mobile router configuration mode. To return the registration parameters to their default settings, use the **no** form of this command.

register {**extend expire** *seconds* **retry** *number* **interval** *seconds* | **lifetime** *seconds* | **retransmit initial** *milliseconds* **maximum** *milliseconds* **retry** *number*}

no register {**extend expire** *seconds* **retry** *number* **interval** *seconds* | **lifetime** *seconds* | **retransmit initial** *milliseconds* **maximum** *milliseconds* **retry** *number*}

Syntax Description

extend	Reregisters before the lifetime expires.
expire *seconds*	Specifies the time (in seconds) in which to send a registration request before expiration. In IPv4, the range is from 1 to 3600; the default is 120. In IPv6, the range is from 1 to 600.
retry *number*	Specifies the number of times the mobile router retries sending a registration request if no reply is received. In both IPv4 and IPv6, the range is from 0 to 10; the default is 3. A value of 0 means no retry. The mobile router stops sending registration requests after the maximum number of retries is attempted.
interval *seconds*	Specifies the time (in seconds) that the mobile router waits before sending another registration request if no reply is received. In IPv4, the range is from 1 to 3600; the default is 10. In IPv6, the range is from 1 to 60.
lifetime *seconds*	Specifies the requested lifetime (in seconds) of each registration. The shortest value between the configured lifetime and the foreign agent advertised registration lifetime is used. In IPv4, the range is from 3 to 65534; the default is 65534 (infinity). In IPv6, the range is from 4 to 262143; the default is 262143 (infinity). This default ensures that the advertised lifetime is used, excluding infinity.
retransmit initial *milliseconds*	Specifies the wait period (in milliseconds) before sending a retransmission the first time no reply is received from the foreign agent. In IPv4, the range is from 10 to 10000 milliseconds (10 seconds); the default is 1000 milliseconds (1 second). In IPv6, the range is from 1000 to 256000.
maximum *milliseconds* **retry** *number*	Specifies the maximum wait period (in milliseconds) before retransmission of a registration request. In IPv4, the range is 10 to 10000 (10 seconds); the default is 5000 milliseconds (5 seconds). In IPv6, the maximum range is from 1000 to 256000. In IPv6, the retry number range is from 0 to 10. Each successive retransmission timeout period is twice the previous period, if the previous period was less than the maximum value. Retransmission stops after the maximum number of retries.

Command Default

The registration parameters of the IPv6 mobile router are used.

Command Modes

Mobile router configuration
IPv6 mobile router configuration (IPv6-mobile-router)

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.4(20)T	Support for IPv6 was added.

Usage Guidelines

The **register lifetime** *seconds* command configures the lifetime that the mobile router requests in a registration request. The home agent also has lifetimes that are set. If the registration request from a mobile router has a greater lifetime than the registration reply from the home agent, the lifetime set on the home agent will be used for the registration. If the registration request lifetime from the mobile router is less than the registration reply from the home agent, the lifetime set on the mobile router will be used. Thus, the smaller lifetime between the home agent and mobile router is used for registration.

Examples

The following example specifies a registration lifetime of 600 seconds:

```
ip mobile router
 address 10.1.1.10 255.255.255.0
 home-agent 10.1.1.20
 register lifetime 600
```

Related Commands

Command	Description
ipv6 mobile router	Enables IPv6 NEMO functionality on the router and places the router in IPv6 mobile router mode.
show ip mobile router	Displays configuration information and monitoring statistics about the mobile router.
show ip mobile router registration	Displays the pending and accepted registrations of the mobile router.

registrar

To enable Session Initiation Protocol (SIP) gateways to register E.164 numbers on behalf of analog telephone voice ports (FXS), IP phone virtual voice ports (EFXS), and Skinny Client Control Protocol (SCCP) phones with an external SIP proxy or SIP registrar, use the **registrar** command in SIP UA configuration mode. To disable registration of E.164 numbers, use the **no** form of this command.

registrar {**dhcp** | [*registrar-index*] *registrar-server-address* [**:***port*]} [**auth-realm** *realm*] [**expires** *seconds*] [**random-contact**] [**refresh-ratio** *ratio-percentage*] [**scheme** {**sip** | **sips**}] [**tcp**] [*type*] [**secondary**]

no registrar [*registrar-index* | **secondary**]

Syntax Description

dhcp	(Optional) Specifies that the domain name of the primary registrar server is retrieved from a DHCP server (cannot be used to configure secondary or multiple registrars).
registrar-index	(Optional) A specific registrar to be configured, allowing configuration of multiple registrars (maximum of six). Range is 1 to 6.
registrar-server-address	The SIP registrar server address to be used for endpoint registration. This value can be entered in one of three formats: • **dns:***address*—the Domain Name System (DNS) address of the primary SIP registrar server (the **dns:** delimiter must be included as the first four characters). • **ipv4:***address*—the IP address of the SIP registrar server (the **ipv4:** delimiter must be included as the first five characters). • **ipv6:[***address*]—the IPv6 address of the SIP registrar server (the **ipv6:** delimiter must be included as the first five characters and the address itself must include opening and closing square brackets).
[**:***port*]	(Optional) The SIP port number (the colon delimiter is required).
auth-realm	(Optional) Specifies the realm for preloaded authorization.
realm	The realm name.
expires *seconds*	(Optional) Specifies the default registration time, in seconds. Range is 60 to 65535. Default is 3600.
random-contact	(Optional) Specifies the Random String Contact header used to identify the registration session.
refresh-ratio *ratio-percentage*	(Optional) Specifies the registration refresh ratio, in percentage. Range is 1 to 100. Default is 80.
scheme {**sip**	**sips**}	(Optional) Specifies the URL scheme. The options are SIP (**sip**) or secure SIP (**sips**), depending on your software installation**.** The default is **sip**.
tcp	(Optional) Specifies TCP. If not specified, the default is User Datagram Protocol UDP.

type	(Optional) The registration type. **Note** The *type* argument cannot be used with the **dhcp** option.
secondary	(Optional) Specifies a secondary SIP registrar for redundancy if the primary registrar fails. This option is not valid if specifying DHCP or if configuring multiple registrars. **Note** You cannot configure any other optional settings once you enter the **secondary** keyword—specify all other settings first.

Command Default

Registration is disabled.

Command Modes

SIP UA configuration (config-sip-ua)

Command History

Release	Modification
12.2(15)ZJ	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4(6)T	This command was modified. The **tls** keyword and the **scheme** keyword with the *string* argument were added.
12.4(22)T	This command was modified. Support for IPv6 addresses was added.
12.4(22)YB	This command was modified. The **dhcp**, **random-contact and refresh-ratio** keywords were added. Additionally, the **aor-domain** keyword and the **tls** option for the **tcp** keyword were removed.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
15.0(1)XA	This command was modified. The *registrar-index* argument for support of multiple registrars on SIP trunks was added.
15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.
15.1(2)T	This command was modified. The **auth-realm** keyword was added.

Usage Guidelines

Use the **registrar dhcp** or **registrar** *registrar-server-address* command to enable the gateway to register E.164 telephone numbers with primary and secondary external SIP registrars. In Cisco IOS Release 15.0(1)XA and later releases, endpoints on Cisco IOS SIP time-division multiplexing (TDM) gateways, Cisco Unified Border Elements (Cisco UBEs), and Cisco Unified Communications Manager Express (Cisco Unified CME) can be registered to multiple registrars using the **registrar** *registrar-index* command.

By default, Cisco IOS SIP gateways do not generate SIP register messages.

Note When entering an IPv6 address, you must include square brackets around the address value.

Examples

The following example shows how to configure registration with a primary and secondary registrar:

```
Router> enable
Router# configure terminal
```

```
Router(config)# sip-ua
Router(config-sip-ua)# retry invite 3
Router(config-sip-ua)# retry register 3
Router(config-sip-ua)# timers register 150
Router(config-sip-ua)# registrar ipv4:209.165.201.1 expires 14400 secondary
```

The following example shows how to configure a device to register with the SIP server address received from the DHCP server. The **dhcp** keyword is available only for configuration by the primary registrar and cannot be used if configuring multiple registrars.

```
Router> enable
Router# configure terminal
Router(config)# sip-ua
Router(config-sip-ua)# registrar dhcp expires 14400
```

The following example shows how to configure a primary registrar using an IP address with TCP:

```
Router> enable
Router# configure terminal
Router(config)# sip-ua
Router(config-sip-ua)# retry invite 3
Router(config-sip-ua)# retry register 3
Router(config-sip-ua)# timers register 150
Router(config-sip-ua)# registrar ipv4:209.165.201.3 tcp
```

The following example shows how to configure a URL scheme with SIP security:

```
Router> enable
Router# configure terminal
Router(config)# sip-ua
Router(config-sip-ua)# retry invite 3
Router(config-sip-ua)# retry register 3
Router(config-sip-ua)# timers register 150
Router(config-sip-ua)# registrar ipv4:209.165.201.7 scheme sips
```

The following example shows how to configure a secondary registrar using an IPv6 address:

```
Router> enable
Router# configure terminal
Router(config)# sip-ua
Router(config-sip-ua)# registrar ipv6:[3FFE:501:FFFF:5:20F:F7FF:FE0B:2972] expires 14400
secondary
```

The following example shows how to configure all POTS endpoints to two registrars using DNS addresses:

```
Router> enable
Router# configure terminal
Router(config)# sip-ua
Router(config-sip-ua)# registrar 1 dns:example1.com expires 180
Router(config-sip-ua)# registrar 2 dns:example2.com expires 360
```

The following example shows how to configure the realm for preloaded authorization using the registrar server address:

```
Router> enable
Router# configure terminal
Router(config)# sip-ua
Router(config-sip-ua)# registrar 2 192.168.140.3:8080 auth-realm example.com expires 180
```

Related Commands

Command	Description
authentication (dial peer)	Enables SIP digest authentication on an individual dial peer.
authentication (SIP UA)	Enables SIP digest authentication.
credentials (SIP UA)	Configures a Cisco UBE to send a SIP registration message when in the UP state.

Command	Description
localhost	Configures global settings for substituting a DNS localhost name in place of the physical IP address in the From, Call-ID, and Remote-Party-ID headers of outgoing messages.
retry register	Sets the total number of SIP register messages to send.
show sip-ua register status	Displays the status of E.164 numbers that a SIP gateway has registered with an external primary or secondary SIP registrar.
timers register	Sets how long the SIP UA waits before sending register requests.
voice-class sip localhost	Configures settings for substituting a DNS localhost name in place of the physical IP address in the From, Call-ID, and Remote-Party-ID headers of outgoing messages on an individual dial peer, overriding the global setting.

remark (IPv6)

To write a helpful comment (remark) for an entry in an IPv6 access list, use the **remark** command in IPv6 access list configuration mode. To remove the remark, use the **no** form of this command.

remark *text-string*

no remark *text-string*

Syntax Description

text-string	Comment that describes the access list entry, up to 100 characters long.

Command Default

IPv6 access list entries have no remarks.

Command Modes

IPv6 access list configuration

Command History

Release	Modification
12.0(23)S	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(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.

Usage Guidelines

The **remark** (IPv6) command is similar to the **remark** (IP) command, except that it is IPv6-specific.

The remark can be up to 100 characters long; anything longer is truncated.

Examples

The following example configures a remark for the IPv6 access list named TELNETTING. The remark is specific to not letting the Marketing subnet use outbound Telnet.

```
ipv6 access-list TELNETTING
 remark Do not allow Marketing subnet to telnet out
 deny tcp 2001:0DB8:0300:0201::/64 any eq telnet
```

Related Commands

Command	Description
ipv6 access-list	Defines an IPv6 access list and enters IPv6 access list configuration mode.
show ipv6 access-list	Displays the contents of all current IPv6 access lists.

retry register

Usage Guidelines

To set the total number of Session Initiation Protocol (SIP) register messages that the gateway should send, use the **retry register** command in SIP user-agent configuration mode. To reset this number to the default, use the **no** form of this command.

retry register *retries* [**exhausted-random-interval minimum** *minutes* **maximum** *minutes*]

no retry register

Syntax Description

retries	Total number of register messages that the gateway should send. The range is from 1 to 10, and the default is 10 retries.
exhausted-random-interval	Specifies that the register request is generated within the defined range of time intervals.
minimum *minutes*	Specifies the minimum time interval range in minutes that will be used as the interval before the next registration is sent.
maximum *minutes*	Specifies the maximum time interval range in minutes that will be used as the interval before the next registration is sent.

Command Default

The gateway sends ten retries.

Command Modes

SIP UA configuration

Command History

Release	Modification
12.2(15)ZJ	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4(22)T	This command was modified. Support for IPv6 was added.
12.4(22)YB	The **exhausted-random-interval** keyword was added.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

Use the default number of 10 when possible. Lower values such as 1 can lead to an increased chance of the message not being received by the other user agent.

Examples

The following example specifies that the gateway sends nine register messages:

```
sip-ua
 retry register 9
```

The following example specifies that the gateway sends six register message, and that a random number, between the 2 and 5 minutes will be used as the interval before the next registration is sent

```
sip-ua
 retry register 6 exhausted-random-interval minimum 2 maximum 5
```

Related Commands

Command	Description
registrar	Enables SIP gateways to register E.164 numbers on behalf of analog telephone voice ports (FXS), IP phone virtual voice ports (EFXS), and SCCP phones with an external SIP proxy or SIP registrar.
timers register	Sets how long the SIP user agent waits before sending register requests.

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.

router bgp

To configure the Border Gateway Protocol (BGP) routing process, use the **router bgp** command in global configuration mode. To remove a BGP routing process, use the **no** form of this command.

router bgp *autonomous-system-number*

no router bgp *autonomous-system-number*

Syntax Description

autonomous-system-number	Number of an autonomous system that identifies the router to other BGP routers and tags the routing information that is passed along. Number in the range from 1 to 65535. • In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, 4-byte autonomous system numbers are supported in the range from 65536 to 4294967295 in asplain notation and in the range from 1.0 to 65535.65535 in asdot notation. • In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, 4-byte autonomous system numbers are supported in the range from 1.0 to 65535.65535 in asdot notation only. For more details about autonomous system number formats, see the "Usage Guidelines" section.

Command Default

No BGP routing process is enabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
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)SRB	This command was modified. Support for IPv6 was added.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX.
12.2(33)SB	This command was modified. Support for IPv6 was added.
12.0(32)S12	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(24)T	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.

Release	Modification
Cisco IOS XE Release 2.3	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SXI1	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
12.2(33)SRE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.

Usage Guidelines

This command allows you to set up a distributed routing core that automatically guarantees the loop-free exchange of routing information between autonomous systems.

Prior to January 2009, BGP autonomous system numbers that were allocated to companies were 2-octet numbers in the range from 1 to 65535 as described in RFC 4271, *A Border Gateway Protocol 4 (BGP-4)*. Due to increased demand for autonomous system numbers, the Internet Assigned Number Authority (IANA) will start in January 2009 to allocate four-octet autonomous system numbers in the range from 65536 to 4294967295. RFC 5396, *Textual Representation of Autonomous System (AS) Numbers*, documents three methods of representing autonomous system numbers. Cisco has implemented the following two methods:

- Asplain—Decimal value notation where both 2-byte and 4-byte autonomous system numbers are represented by their decimal value. For example, 65526 is a 2-byte autonomous system number and 234567 is a 4-byte autonomous system number.
- Asdot—Autonomous system dot notation where 2-byte autonomous system numbers are represented by their decimal value and 4-byte autonomous system numbers are represented by a dot notation. For example, 65526 is a 2-byte autonomous system number and 1.169031 is a 4-byte autonomous system number (this is dot notation for the 234567 decimal number).

For details about the third method of representing autonomous system numbers, see RFC 5396.

Note In Cisco IOS releases that include 4-byte ASN support, command accounting and command authorization that include a 4-byte ASN number are sent in the asplain notation irrespective of the format that is used on the command-line interface.

Asdot Only Autonomous System Number Formatting

In Cisco IOS Release 12.0(32)S12, 12.4(24)T, Cisco IOS XE Release 2.3, and later releases, the 4-octet (4-byte) autonomous system numbers are entered and displayed only in asdot notation, for example, 1.10 or 45000.64000. When using regular expressions to match 4-byte autonomous system numbers the asdot format includes a period which is a special character in regular expressions. A backslash must be entered before the period for example, 1\.14, to ensure the regular expression match does not fail. Table 46 shows

the format in which 2-byte and 4-byte autonomous system numbers are configured, matched in regular expressions, and displayed in **show** command output in Cisco IOS images where only asdot formatting is available.

Table 46 Asdot Only 4-Byte Autonomous System Number Format

Format	Configuration Format	Show Command Output and Regular Expression Match Format
asdot	2-byte: 1 to 65535 4-byte: 1.0 to 65535.65535	2-byte: 1 to 65535 4-byte: 1.0 to 65535.65535

Asplain as Default Autonomous System Number Formatting

In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, the Cisco implementation of 4-byte autonomous system numbers uses asplain as the default display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain and asdot format. In addition, the default format for matching 4-byte autonomous system numbers in regular expressions is asplain, so you must ensure that any regular expressions to match 4-byte autonomous system numbers are written in the asplain format. If you want to change the default **show** command output to display 4-byte autonomous system numbers in the asdot format, use the **bgp asnotation dot** command under router configuration mode. When the asdot format is enabled as the default, any regular expressions to match 4-byte autonomous system numbers must be written using the asdot format, or the regular expression match will fail. Table 47 and Table 48 show that although you can configure 4-byte autonomous system numbers in either asplain or asdot format, only one format is used to display **show** command output and control 4-byte autonomous system number matching for regular expressions, and the default is asplain format. To display 4-byte autonomous system numbers in **show** command output and to control matching for regular expressions in the asdot format, you must configure the **bgp asnotation dot** command. After enabling the **bgp asnotation dot** command, a hard reset must be initiated for all BGP sessions by entering the **clear ip bgp *** command.

Note If you are upgrading to an image that supports 4-byte autonomous system numbers, you can still use 2-byte autonomous system numbers. The **show** command output and regular expression match are not changed and remain in asplain (decimal value) format for 2-byte autonomous system numbers regardless of the format configured for 4-byte autonomous system numbers.

Table 47 Default Asplain 4-Byte Autonomous System Number Format

Format	Configuration Format	Show Command Output and Regular Expression Match Format
asplain	2-byte: 1 to 65535 4-byte: 65536 to 4294967295	2-byte: 1 to 65535 4-byte: 65536 to 4294967295
asdot	2-byte: 1 to 65535 4-byte: 1.0 to 65535.65535	2-byte: 1 to 65535 4-byte: 65536 to 4294967295

Table 48 Asdot 4-Byte Autonomous System Number Format

Format	Configuration Format	Show Command Output and Regular Expression Match Format
asplain	2-byte: 1 to 65535 4-byte: 65536 to 4294967295	2-byte: 1 to 65535 4-byte: 1.0 to 65535.65535
asdot	2-byte: 1 to 65535 4-byte: 1.0 to 65535.65535	2-byte: 1 to 65535 4-byte: 1.0 to 65535.65535

Reserved and Private Autonomous System Numbers

In Cisco IOS Release 12.0(32)S12, 12.0(32)SY8, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, 12.4(24)T, Cisco IOS XE Release 2.3 and later releases, the Cisco implementation of BGP supports RFC 4893. RFC 4893 was developed to allow BGP to support a gradual transition from 2-byte autonomous system numbers to 4-byte autonomous system numbers. A new reserved (private) autonomous system number, 23456, was created by RFC 4893 and this number cannot be configured as an autonomous system number in the Cisco IOS CLI.

RFC 5398, *Autonomous System (AS) Number Reservation for Documentation Use*, describes new reserved autonomous system numbers for documentation purposes. Use of the reserved numbers allow configuration examples to be accurately documented and avoids conflict with production networks if these configurations are literally copied. The reserved numbers are documented in the IANA autonomous system number registry. Reserved 2-byte autonomous system numbers are in the contiguous block, 64496 to 64511 and reserved 4-byte autonomous system numbers are from 65536 to 65551 inclusive.

Private 2-byte autonomous system numbers are still valid in the range from 64512 to 65534 with 65535 being reserved for special use. Private autonomous system numbers can be used for internal routing domains but must be translated for traffic that is routed out to the Internet. BGP should not be configured to advertise private autonomous system numbers to external networks. Cisco IOS software does not remove private autonomous system numbers from routing updates by default. We recommend that ISPs filter private autonomous system numbers.

Note Autonomous system number assignment for public and private networks is governed by the IANA. For information about autonomous-system numbers, including reserved number assignment, or to apply to register an autonomous system number, see the following URL: http://www.iana.org/.

Examples

The following example configures a BGP process for autonomous system 45000 and configures two external BGP neighbors in different autonomous systems using 2-byte autonomous system numbers:

```
router bgp 45000
 neighbor 192.168.1.2 remote-as 40000
 neighbor 192.168.3.2 remote-as 50000
 neighbor 192.168.3.2 description finance
 !
 address-family ipv4
  neighbor 192.168.1.2 activate
  neighbor 192.168.3.2 activate
  no auto-summary
  no synchronization
  network 172.17.1.0 mask 255.255.255.0
  exit-address-family
```

The following example configures a BGP process for autonomous system 65538 and configures two external BGP neighbors in different autonomous systems using 4-byte autonomous system numbers in asplain notation. This example is supported in Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases.

```
router bgp 65538
 neighbor 192.168.1.2 remote-as 65536
 neighbor 192.168.3.2 remote-as 65550
 neighbor 192.168.3.2 description finance
 !
 address-family ipv4
  neighbor 192.168.1.2 activate
  neighbor 192.168.3.2 activate
  no auto-summary
  no synchronization
  network 172.17.1.0 mask 255.255.255.0
  exit-address-family
```

The following example configures a BGP process for autonomous system 1.2 and configures two external BGP neighbors in different autonomous systems using 4-byte autonomous system numbers in asdot notation. This example is supported in Cisco IOS Release 12.0(32)SY8, 12.0(32)S12, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, 12.4(24)T, and Cisco IOS XE Release 2.3, and later releases.

```
router bgp 1.2
 neighbor 192.168.1.2 remote-as 1.0
 neighbor 192.168.3.2 remote-as 1.14
 neighbor 192.168.3.2 description finance
 !
 address-family ipv4
  neighbor 192.168.1.2 activate
  neighbor 192.168.3.2 activate
  no auto-summary
  no synchronization
  network 172.17.1.0 mask 255.255.255.0
  exit-address-family
```

Related Commands

Command	Description
bgp asnotation dot	Changes the default display and the regular expression match format of BGP 4-byte autonomous system numbers from asplain (decimal values) to dot notation.
neighbor remote-as	Adds an entry to the BGP or multiprotocol BGP neighbor table.
network (BGP and multiprotocol BGP)	Specifies the list of networks for the BGP routing process.

router ospfv3

To enter Open Shortest Path First version 3 (OSPFv3) router configuration mode , use the **router ospfv3** command in interface configuration mode.

router ospfv3 [*process-id*]

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.

Command Default

No OSPFv3 routing process is defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

Use the **router ospfv3** command to enter the OSPFv3 router configuration mode. From this mode, you can enter address-family configuration mode for IPv6 or IPv4 and then configure the IPv6 or IPv4 AF.

Examples

The following example enters OSPFv3 router configuration mode:

```
Router(config)# router ospfv3 1
Router(config-router)#
```

Related Commands

Command	Description
ipv6 ospf area	Enables OSPFv3 on an interface
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

route-map

To define the conditions for redistributing routes from one routing protocol into another routing protocol, or to enable policy routing, use the **route-map** command in global configuration mode and the **match** and **set** commands in route-map configuration modes. To delete an entry, use the **no** form of this command.

route-map *map-tag* [**permit** | **deny**] [*sequence-number*]

no route-map *map-tag* [**permit** | **deny**] [*sequence-number*]

Syntax Description

map-tag	A meaningful name for the route map. The **redistribute** router configuration command uses this name to reference this route map. Multiple route maps may share the same map tag name.
permit	(Optional) If the match criteria are met for this route map, and the **permit** keyword is specified, the route is redistributed as controlled by the set actions. In the case of policy routing, the packet is policy routed. If the match criteria are not met, and the **permit** keyword is specified, the next route map with the same map tag is tested. If a route passes none of the match criteria for the set of route maps sharing the same name, it is not redistributed by that set.
deny	(Optional) If the match criteria are met for the route map and the **deny** keyword is specified, the route is not redistributed. In the case of policy routing, the packet is not policy routed, and no further route maps sharing the same map tag name will be examined. If the packet is not policy routed, the normal forwarding algorithm is used.
sequence-number	(Optional) Number that indicates the position a new route map will have in the list of route maps already configured with the same name. If used with the **no** form of this command, the position of the route map should be deleted.

Command Default

Policy routing is not enabled and conditions for redistributing routes from one routing protocol into another routing protocol are not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.3(7)T	This command was updated for use in configuring IPv6 policy-based routing (PBR).
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Release	Modification
Cisco IOS XE Release 2.1	This command was implemented on Cisco ASR 1000 Series Aggregation Services Routers.
12.2(33)SXI4	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SXI4.

Usage Guidelines

Use the **route-map** command to enter route-map configuration mode.

Use route maps to redistribute routes or to subject packets to policy routing. Both purposes are described in this section.

Redistribution

Use the **route-map** global configuration command, and the **match** and **set** route-map configuration commands, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the *set actions*—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **match** route-map configuration command has multiple formats. The **match** commands can be given in any order, and all **match** commands must "pass" to cause the route to be redistributed according to the *set actions* given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

Use route maps when you want detailed control over how routes are redistributed between routing processes. The destination routing protocol is the one you specify with the **router** global configuration command. The source routing protocol is the one you specify with the **redistribute** router configuration command. See the "Examples" section for an illustration of how route maps are configured.

When you are passing routes through a route map, a route map can have several parts. Any route that does not match at least one **match** clause relating to a **route-map** command will be ignored; that is, the route will not be advertised for outbound route maps and will not be accepted for inbound route maps. If you want to modify only some data, you must configure a second route map section with an explicit match specified.

Policy Routing

Another purpose of route maps is to enable policy routing. Use the **ip policy route-map** or **ipv6 policy route-map** command, in addition to the **route-map** command, and the **match** and **set** commands to define the conditions for policy routing packets. The **match** commands specify the conditions under which policy routing occurs. The **set** commands specify the routing actions to perform if the criteria enforced by the **match** commands are met. You might want to policy route packets some way other than the obvious shortest path.

The *sequence-number* argument works as follows:

1. If no entry is defined with the supplied tag, an entry is created with the *sequence-number* argument set to 10.
2. If only one entry is defined with the supplied tag, that entry becomes the default entry for the following **route-map** command. The *sequence-number* argument of this entry is unchanged.
3. If more than one entry is defined with the supplied tag, an error message is printed to indicate that the *sequence-number* argument is required.

If the **no route-map** *map-tag* command is specified (with no *sequence-number* argument), the whole route map is deleted.

Examples

The following example redistributes Routing Information Protocol (RIP) routes with a hop count equal to 1 into Open Shortest Path First (OSPF). These routes will be redistributed into OSPF as external link-state advertisements (LSAs) with a metric of 5, metric type of Type 1, and a tag equal to 1.

```
Router(config)# router ospf 109
Router(config-router)# redistribute rip route-map rip-to-ospf
Router(config-router)# exit
Router(config)# route-map rip-to-ospf permit
Router(config-route-map)# match metric 1
Router(config-route-map)# set metric 5
Router(config-route-map)# set metric-type type1
Router(config-route-map)# set tag 1
```

The following example for IPv6 redistributes RIP routes with a hop count equal to 1 into OSPF. These routes will be redistributed into OSPF as external LSAs with a tag equal to 42 and a metric type equal to type1.

```
Router(config)# ipv6 router ospf 1
Router(config-router)# redistribute rip one route-map rip-to-ospfv3
Router(config-router)# exit
Router(config)# route-map rip-to-ospfv3
Router(config-route-map)# match tag 42
Router(config-route-map)# set metric-type type1
```

The following named configuration example redistributes Enhanced Interior Gateway Routing Protocol (EIGRP) addresses with a hop count equal to 1. These addresses are redistributed into EIGRP as external with a metric of 5 and a tag equal to 1:

```
Router(config)# router eigrp virtual-name1
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# topology base
Router(config-router-af-topology)# redistribute eigrp 6473 route-map
virtual-name1-to-virtual-name2
Router(config-router-af-topology)# exit-address-topology
Router(config-router-af)# exit-address-family
Router(config-router)# router eigrp virtual-name2
Router(config-router)# address-family ipv4 autonomous-system 6473
Router(config-router-af)# topology base
Router(config-router-af-topology)# exit-af-topology
Router(config-router-af)# exit-address-family
Router(config)# route-map virtual-name1-to-virtual-name2
Router(config-route-map)# match tag 42
Router(config-route-map)# set metric 5
Router(config-route-map)# set tag 1
```

Related Commands

Command	Description
ip policy route-map	Identifies a route map to use for policy routing on an interface.
ipv6 policy route-map	Configures IPv6 PBR on an interface.
match as-path	Matches a BGP autonomous system path access list.
match community	Matches a BGP community.
match interface (IP)	Distributes any routes that have their next hop out one of the interfaces specified.

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, and performs policy routing on packets.
match ipv6 address	Distributes IPv6 routes that have a prefix permitted by a prefix list or to specify an IPv6 access list to use to match packets for PBR for IPv6.
match ip next-hop	Redistributes any routes that have a next hop router address passed by one of the access lists specified.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match length	Bases policy routing on the Level 3 length of a packet.
match metric (IP)	Redistributes routes with the metric specified.
match route-type (IP)	Redistributes routes of the specified type.
match tag	Redistributes routes in the routing table that match the specified tags.
router eigrp	Configures the EIGRP address-family process.
set as-path	Modifies an autonomous system path for BGP routes.
set automatic-tag	Automatically computes the tag value.
set community	Sets the BGP communities attribute.
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Indicates where to output packets that pass a match clause of a route map for policy routing.
set ipv6 default next-hop	Specifies an IPv6 default next hop to which matching packets will be forwarded.
set ip default next-hop verify-availability	Indicates where to output packets that pass a match clause of a route map for policy routing and for which the Cisco IOS software has no explicit route to a destination.
set ip next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing.
set ipv6 next-hop (PBR)	Indicates where to output IPv6 packets that pass a match clause of a route map for PBR for IPv6.
set level (IP)	Indicates where to import routes.
set local preference	Specifies a preference value for the autonomous system path.
set metric (BGP, OSPF, RIP)	Sets the metric value for a routing protocol.
set metric type	Sets the metric type for the destination routing protocol.
set next-hop	Specifies the address of the next hop.
set tag (IP)	Sets a tag value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.
show route-map	Displays all route maps configured or only the one specified.

router-id (IPv6)

To use a fixed router ID, use the **router-id** command in router configuration mode. To force Open Shortest Path First (OSPF) for IPv6 to use the previous OSPF for IPv6 router ID behavior, use the **no** form of this command.

router-id {*router-id*}

no router-id {*router-id*}

Syntax Description

router-id	Router ID for this OSPF process.

Command Default

The router ID is chosen automatically.

Command Modes

Router configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.4(6)T	Support for Enhanced Internal Gateway Routing Protocol (EIGRP) IPv6 was added.
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.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 series routers.

Usage Guidelines

OSPF for IPv6 (or OSPF version 3, or OSPFv3) is backward-compatible with OSPF version 2. In OSPFv3 and OSPF version 2, the router uses the 32-bit IPv4 address to select the router ID for an OSPF process. If an IPv4 address exists when OSPFv3 is enabled on an interface, then that IPv4 address is used for the router ID. If more than one IPv4 address is available, a router ID is chosen using the same rules as for OSPF version 2. If no IPv4 addresses are configured, the router selects a router ID automatically. Each router ID must be unique.

If this command is used on an OSPF for IPv6 router process that is already active (has neighbors), the new router ID is used at the next reload or at a manual OSPFv3 process restart. To manually restart the OSPFv3 process, use the **clear ipv6 ospf process** command.

Examples

The following example specifies a fixed router ID:

```
Router(config-rtr)# router-id 10.1.1.1
```

Related Commands

Command	Description
clear ipv6 ospf	Clears the OSPF for IPv6 state based on the OSPF routing process ID.
ipv6 router eigrp	Configures the EIGRP IPv6 routing process.
ipv6 router ospf	Enables OSPF for IPv6 router configuration mode.

router-id (OSPFv3)

To use a fixed router ID, use the **router-id** command in Open Shortest Path First version 3 (OSPFv3) router configuration mode. To force OSPFv3 to use the previous OSPFv3 router ID behavior in IPv4, use the **no** form of this command.

router-id {*router-id*}

no router-id {*router-id*}

Syntax Description

router-id	Router ID for this OSPFv3 process.

Command Default

The router ID is chosen automatically.

Command Modes

OSPFv3 router configuration mode (config-router)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

OSPFv3 is backward-compatible with OSPF version 2. In OSPFv3 and OSPF version 2, the router uses the 32-bit IPv4 address to select the router ID for an OSPFv3 process. If an IPv4 address exists when OSPFv3 is enabled on an interface, then that IPv4 address is used for the router ID. If more than one IPv4 address is available, a router ID is chosen using the same rules as for OSPF version 2. If no IPv4 addresses are configured, the router selects a router ID automatically. Each router ID must be unique.

If this command is used on an OSPFv3 router process that is already active (has neighbors), the new router ID is used at the next reload or at a manual OSPFv3 process restart.

Examples

The following example specifies a fixed router ID:

```
Router(config-router)# router-id 10.1.1.1
```

Related Commands

Command	Description
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

router-preference maximum

To verify the advertised default router preference parameter value, use the **router-preference maximum** command in router advertisement (RA) guard policy configuration mode:

router-preference maximum {**high** | **low** | **medium**}

Syntax Description

high	Default router preference parameter value is higher than the specified limit.
medium	Default router preference parameter value is equal to the specified limit.
low	Default router preference parameter value is lower than the specified limit.

Command Default

The router preference maximum value is not configured.

Command Modes

RA guard policy configuration (config-ra-guard)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

The **router-preference maximum** command enables verification that the advertised default router preference parameter value is lower than or equal to a specified limit. You can use this command to give a lower priority to default routers advertised on trunk ports, and to give precedence to default router advertised on access ports.

The **router-preference maximum** command limit are high, medium, or low. If, for example, this value is set to **medium** and the advertised **default router preference** is set to **high** in the received packet, then packet is dropped. If the command option is set to **medium** or **low** in the received packet, then packet is not dropped.

Examples

The following example defines an RA guard policy name as raguard1, places the router in RA guard policy configuration mode, and configures router-preference maximum verification to be high:

```
Router(config)# ipv6 nd raguard policy raguard1
Router(config-nd-inspection)# router-preference maximum high
```

Related Commands

Command	Description
ipv6 nd raguard policy	Defines the RA guard policy name and enter RA guard policy configuration mode.

route-target

To create a route-target extended community for a Virtual Private Network (VPN) routing and forwarding (VRF) instance, use the **route-target** command in VRF configuration or in VRF address family configuration mode. To disable the configuration of a route-target community option, use the **no** form of this command.

route-target [**import** | **export** | **both**] *route-target-ext-community*

no route-target [**import** | **export** | **both**] [*route-target-ext-community*]

Syntax Description

import	(Optional) Imports routing information from the target VPN extended community.
export	(Optional) Exports routing information to the target VPN extended community.
both	(Optional) Imports both import and export routing information to the target VPN extended community.
route-target-ext-community	The route-target extended community attributes to be added to the VRF's list of import, export, or both (import and export) route-target extended communities.

Command Default

A VRF has no route-target extended community attributes associated with it.

Command Modes

VRF address family configuration (config-vrf-af)
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(14)S	This command was integrated into Cisco IOS 12.2(14)S.
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)SRB	This command was modified. Support for IPv6 was added.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
12.0(32)S12	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(24)T	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.

Release	Modification
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
Cisco IOS XE Release 2.3	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SXI1	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers was changed to asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers was changed to asplain.
12.2(33)SRE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.

Usage Guidelines

The **route-target** command creates lists of import and export route-target extended communities for the specified VRF. Enter the command one time for each target community. Learned routes that carry a specific route-target extended community are imported into all VRFs configured with that extended community as an import route target. Routes learned from a VRF site (for example, by Border Gateway Protocol (BGP), Routing Information Protocol (RIP), or static route configuration) contain export route targets for extended communities configured for the VRF added as route attributes to control the VRFs into which the route is imported.

The route target specifies a target VPN extended community. Like a route distinguisher, an extended community is composed of either an autonomous system number and an arbitrary number or an IP address and an arbitrary number. You can enter the numbers 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.

Note In Cisco IOS releases that include 4-byte ASN support, command accounting and command authorization that include a 4-byte ASN number are sent in the asplain notation irrespective of the format that is used on the command-line interface.

In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, the Cisco implementation of 4-byte autonomous system numbers uses asplain—65538, for example—as the default regular expression match and output display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain format and the asdot format as described in RFC 5396. To change the default regular expression match and output display of 4-byte autonomous system numbers to asdot format, use the **bgp asnotation dot** command followed by the **clear ip bgp *** command to perform a hard reset of all current BGP sessions.

In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, the Cisco implementation of 4-byte autonomous system numbers uses asdot—1.2, for example—as the only configuration format, regular expression match, and output display, with no asplain support.

Examples

The following example shows how to configure route-target extended community attributes for a VRF in IPv4. The result of the command sequence is that VRF named vrf1 has two export extended communities (1000:1 and 1000:2) and two import extended communities (1000:1 and 10.27.0.130:200):

```
ip vrf vrf1
 route-target both 1000:1
 route-target export 1000:2
 route-target import 10.27.0.130:200
```

The following example shows how to configure route-target extended community attributes for a VRF that includes IPv4 and IPv6 address families:

```
vrf definition site1
rd 1000:1
address-family ipv4
 route-target export 100:1
 route-target import 100:1
address-family ipv6
 route-target export 200:1
 route-target import 200:1
```

The following example available in Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases shows how to create a VRF with a route target that uses a 4-byte autonomous system number in asplain format—65537—and how to set the route target to extended community value 65537:100 for routes that are permitted by the route map:

```
ip vrf vrf1
 rd 64500:100
 route-target both 65537:100
 exit
route-map vrf1 permit 10
 set extcommunity rt 65537:100
 end
```

After the configuration is completed, use the **show route-map** command to verify that the extended community is set to the route target containing the 4-byte autonomous system number of 65537:

```
Router# show route-map vrf1

route-map vrf1, permit, sequence 10
  Match clauses:
  Set clauses:
    extended community RT:65537:100
  Policy routing matches: 0 packets, 0 bytes
```

The following example available in Cisco IOS Release 12.0(32)SY8, 12.0(32)S12, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, 12.4(24)T, Cisco IOS XE Release 2.3, and later releases, shows how to create a VRF with a route target that uses a 4-byte autonomous system number in asdot format—1.1—and how to set the route target to extended community value 1.1:100 for routes that are permitted by the route map:

```
ip vrf vrf1
 rd 64500:100
 route-target both 1.1:100
 exit
```

```
route-map vrf1 permit 10
 set extcommunity rt 1.1:100
 end
```

Related Commands

Command	Description
address-family (VRF)	Selects an address family type for a VRF table and enters VRF address family configuration mode.
bgp asnotation dot	Changes the default display and the regular expression match format of BGP 4-byte autonomous system numbers from asplain (decimal values) to dot notation.
clear ip bgp	Resets Border Gateway Protocol (BGP) connections using hard or soft reconfiguration.
import map	Configures an import route map for a VRF.
ip vrf	Configures a VRF routing table.
vrf definition	Configures a VRF routing table and enters VRF configuration mode.

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.

sccp ccm

To add a Cisco Unified Communications Manager server to the list of available servers and set various parameters—including IP address or Domain Name System (DNS) name, port number, and version number—use the **sccp ccm** command in global configuration mode. To remove a particular server from the list, use the **no** form of this command.

NM-HDV or NM-HDV-FARM Voice Network Modules

sccp ccm {*ipv4-address* | *ipv6-address* | *dns*} **priority** *priority* [**port** *port-number*] [**version** *version-number*] [**trustpoint** *label*]

no sccp ccm {*ipv4-address* | *ipv6-address* | *dns*}

NM-HDV2 or NM-HD-1V/2V/2VE Voice Network Modules

sccp ccm {*ipv4-address* | *ipv6-address* | *dns*} **identifier** *identifier-number* [**priority** *priority*] [**port** *port-number*] [**version** *version-number*] [**trustpoint** *label*]

no sccp ccm {*ipv4-address* | *ipv6-address* | *dns*}

Syntax Description

ipv4-address	IPv4 address of the Cisco Unified Communications Manager server.
ipv6-address	IPv6 address of the Cisco Unified Communications Manager server.
dns	DNS name.
identifier *identifier-number*	Specifies the number that identifies the Cisco Unified Communications Manager server. The range is 1 to 65535.
priority *priority*	Specifies the priority of this Cisco Unified Communications Manager server relative to other connected servers. The range is 1 (highest) to 4 (lowest). **Note** This keyword is required only for NM-HDV and NM-HDV-FARM modules. Do not use this keyword if you are using the NM-HDV2 or NM-HD-1V/2V/2VE; set the priority using the **associate ccm** command in the Cisco Unified Communications Manager group.
port *port-number*	(Optional) Specifies the TCP port number. The range is 1025 to 65535. The default is 2000.
version *version-number*	(Optional) Cisco Unified Communications Manager version. Valid versions are **3.0**, **3.1**, **3.2**, **3.3**, **4.0**, **4.1**, **5.0.1**, **6.0**, and **7.0+**. There is no default value.
trustpoint	(Optional) Specifies the trustpoint for Cisco Unified Communications Manager certificate.
label	Cisco Unified Communications Manager trustpoint label.

Command Default

The default port number is 2000.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(5)YH	This command was introduced.
12.3(8)T	This command was modified. The **identifier** keyword and additional values for Cisco Unified Communications Manager versions were added.
12.4(11)XW	This command was modified. The **6.0** keyword was added to the list of version values.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.4(22)T	This command was modified. Support for IPv6 was added. The **version** keyword and *version-number* argument were changed from being optional to being required, and the **7.0+** keyword was added.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The **trustpoint** keyword and the *label* argument were added.

Usage Guidelines

You can configure up to four Cisco Unified Communications Manager servers—a primary and up to three backups—to support digital signal processor (DSP) farm services. To add the Cisco Unified Communications Manager server to a Cisco Unified Communications Manager group, use the **associate ccm** command.

IPv6 support is provided for registration with Cisco Unified CM version 7.0 and later.

To enable Ad Hoc or Meet-Me hardware conferencing in Cisco Unified CME, you must first set the **version** keyword to **4.0** or a later version.

Beginning with Cisco IOS Release 12.4(22)T users manually configuring the **sccp ccm** command must provide the version. Existing router configurations are not impacted because automatic upgrade and downgrade are supported.

Examples

The following example shows how to add the Cisco Unified Communications Manager server with IP address 10.0.0.0 to the list of available servers:

```
Router(config)# sccp ccm 10.0.0.0 identifier 3 port 1025 version 4.0
```

The following example shows how to add the Cisco Unified CallManager server whose IPv6 address is 2001:DB8:C18:1::102:

```
Router(config)# sccp ccm 2001:DB8:C18:1::102 identifier 2 version 7.0
```

Related Commands

Command	Description
associate ccm	Associates a Cisco Unified Communications Manager server with a Cisco Unified Communications Manager group and establishes its priority within the group.
sccp	Enables SCCP and its associated transcoding and conferencing applications.
sccp ccm group	Creates a Cisco Unified Communications Manager group and enters SCCP Cisco Unified Communications Manager configuration mode.

Command	Description
sccp local	Selects the local interface that SCCP applications use to register with Cisco Unified Communications Manager.
show sccp	Displays SCCP configuration information and current status.

sccp ccm group

To create a Cisco Unified Communications Manager group and enter SCCP Cisco CallManager configuration mode, use the **sccp ccm group** command in global configuration mode. To remove a particular Cisco Unified Communications Manager group, use the **no** form of this command.

sccp ccm group *group-number*

no sccp ccm group *group-number*

Syntax Description

group-number	Number that identifies the Cisco Unified Communications Manager group. Range is 1 to 50.

Command Default

No groups are defined, so all servers are configured individually.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4(22)T	This command was modified. Support for IPv6 was added.
15.0(1)M	This command was modified. The group number range was increased to 50.

Usage Guidelines

Use this command to group Cisco Unified Communications Manager servers that are defined using the **sccp ccm** command. You can associate designated DSP farm profiles using the **associate profile** command so that the DSP services are controlled by the Cisco Unified Communications Manager servers in the group.

Examples

The following example enters SCCP Cisco CallManager configuration mode and associates Cisco Unified Communications Manager 25 with Cisco Unified Communications Manager group 10:

```
Router(config)# sccp ccm group 10
Router(config-sccp-ccm)# associate ccm 25 priority 2
```

Related Commands

Command	Description
associate ccm	Associates a Cisco Unified Communications Manager server with a Cisco Unified Communications Manager group and establishes its priority within the group.
associate profile	Associates a DSP farm profile with a Cisco Unified Communications Manager group.
bind interface	Binds an interface with a Cisco Unified Communications Manager group.

Command	Description
connect interval	Specifies the amount of time that a DSP farm profile waits before attempting to connect to a Cisco Unified Communications Manager when the current Cisco Unified Communications Manager fails to connect.
connect retries	Specifies the number of times that a DSP farm attempts to connect to a Cisco Unified Communications Manager when the current Cisco Unified Communications Manager connections fails.
sccp ccm	Adds a Cisco Unified Communications Manager server to the list of available servers.

sec-level minimum

To specify the minimum security level parameter value when Cryptographically Generated Address (CGA) options are used, use the **sec-level minimum** command in Neighbor Discovery (ND) inspection policy configuration mode. To disable this function, use the **no** form of this command.

sec-level minimum *value*

no sec-level minimum *value*

Syntax Description

value	Sets the minimum security level, which is a value from 1 through 7. The default security level is 1. The most secure level is 3.

Command Default

The default security level is 1.

Command Modes

ND inspection policy configuration (config-nd-inspection)
RA guard policy configuration (config-ra-guard)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

The **sec-level minimum** command specifies the minimum security level parameter value when CGA options are used. Use the **sec-level minimum** command after enabling ND inspection policy configuration mode using the **ipv6 nd inspection policy** command.

Examples

The following example defines an ND policy name as policy1, places the router in ND inspection policy configuration mode, and enables the router to specify 2 as the minimum CGA security level:

```
Router(config)# ipv6 nd inspection policy policy1
Router(config-nd-inspection)# sec-level minimum 2
```

Related Commands

Command	Description
ipv6 nd inspection policy	Defines the ND inspection policy name and enters ND inspection policy configuration mode.
ipv6 nd raguard policy	Defines the RA guard policy name and enter RA guard policy configuration mode.

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.

send-lifetime

To set the time period during which an authentication key on a key chain is valid to be sent, use the **send-lifetime** command in key chain key configuration mode. To revert to the default value, use the **no** form of this command.

send-lifetime *start-time* {**infinite** | *end-time* | **duration** *seconds*}

no send-lifetime [*start-time* {**infinite** | *end-time* | **duration** *seconds*}]

Syntax Description

start-time	Beginning time that the key specified by the **key** command is valid to be sent. The syntax can be either of the following: *hh*:*mm*:*ss Month date year* *hh*:*mm*:*ss date Month year* • *hh*—hours • *mm*—minutes • *ss*—seconds • *Month*—first three letters of the month • *date*—date (1–31) • *year*—year (four digits) The default start time and the earliest acceptable date is January 1, 1993.
infinite	Key is valid to be sent from the *start-time* value on.
end-time	Key is valid to be sent from the *start-time* value until the *end-time* value. The syntax is the same as that for the *start-time* value. The *end-time* value must be after the *start-time* value. The default end time is an infinite time period.
duration *seconds*	Length of time (in seconds) that the key is valid to be sent.

Command Default

Forever (the starting time is January 1, 1993, and the ending time is infinite)

Command Modes

Key chain key configuration (config-keychain-key)

Command History

Release	Modification
11.1	This command was introduced.
12.4(6)T	Support for IPv6 was added.
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.

Usage Guidelines

Specify a *start-time* value and one of the following values: **infinite**, *end-time*, or **duration** *seconds*.

We recommend running Network Time Protocol (NTP) or some other time synchronization method if you intend to set lifetimes on keys.

If the last key expires, authentication will continue and an error message will be generated. To disable authentication, you must manually delete the last valid key.

Examples

The following example configures a key chain named chain1. The key named key1 will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. The key named key2 will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or a discrepancy in the set time of the router. There is a 30-minute leeway on each side to handle time differences.

```
Router(config)# interface ethernet 0
Router(config-if)# ip rip authentication key-chain chain1
Router(config-if)# ip rip authentication mode md5
!
Router(config)# router rip
Router(config-router)# network 172.19.0.0
Router(config-router)# version 2
!
Router(config)# key chain chain1
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string key1
Router(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 14:00:00 Jan 25 1996 duration 3600
Router(config-keychain-key)# exit
Router(config-keychain)# key 2
Router(config-keychain-key)# key-string key2
Router(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 15:00:00 Jan 25 1996 duration 3600
```

The following example configures a key chain named chain1 for EIGRP address-family. The key named key1 will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. The key named key2 will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or a discrepancy in the set time of the router. There is a 30-minute leeway on each side to handle time differences.

```
Router(config)# eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# network 10.0.0.0
Router(config-router-af)# af-interface ethernet0/0
Router(config-router-af-interface)# authentication key-chain trees
Router(config-router-af-interface)# authentication mode md5
Router(config-router-af-interface)# exit
Router(config-router-af)# exit
Router(config-router)# exit
Router(config)# key chain chain1
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string key1
Router(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 14:00:00 Jan 25 1996 duration 3600
Router(config-keychain-key)# exit
Router(config-keychain)# key 2
Router(config-keychain-key)# key-string key2
Router(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 15:00:00 Jan 25 1996 duration 3600
```

Related Commands

Command	Description
accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.
key	Identifies an authentication key on a key chain.
key chain	Defines an authentication key chain needed to enable authentication for routing protocols.
key-string (authentication)	Specifies the authentication string for a key.
show key chain	Displays authentication key information.

send-nat-address

To send a client's post-Network Address Translation (NAT) address to the TACACS+ server, use the **send-nat-address** command in TACACS+ server configuration mode. To disable sending the post-NAT address, use the **no** form of this command.

send-nat-address

no send-nat-address

Syntax Description

This command has no arguments or keywords.

Command Default

The post-NAT address is not sent.

Command Modes

TACACS+ server configuration (config-server-tacacs)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines

Use the **send-nat-address** command to send a client's post-NAT address to the TACACS+ server.

Examples

The following example shows how to send a client's post-NAT address to the TACACS+ server:

```
Router(config)# tacacs server server1
Router(config-server-tacacs)# send-nat-address
```

Related Commands

Command	Description
tacacs server	Configures the TACACS+ server for IPv6 or IPv4 and enters TACACS server configuration mode.

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.

server name (IPv6 TACACS+)

To specify an IPv6 TACACS+ server, use the **server name** command in TACACS+ group server configuration mode. To remove the IPv6 TACACS+ server from configuration, use the **no** form of this command.

server name *server-name*

no server name *server-name*

Syntax Description

server-name	The IPv6 TACACS+ server to be used.

Command Default

No server name is specified.

Command Modes

TACACS+ group server configuration (config-sg-tacacs+)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines

You must configure the **aaa group server tacacs** command before configuring this command.

Enter the **server name** command to specify an IPv6 TACACS+ server.

Examples

The following example shows how to specify an IPv6 TACACS+ server named server1:

```
Router(config)# aaa group server tacacs+
Router(config-sg-tacacs+)# server name server1
```

Related Commands

Command	Description
aaa group server tacacs	Configures the TACACS+ server for IPv6 or IPv4 and enters TACACS+ server configuration mode.

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 IPv4 or IPv6 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* | *ipv6-address*} [**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.
ipv6-address	IPv6 address of the private RADIUS or TACACS+ server host.
nat	(Optional) Specifies the 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.

Release	Modification
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.
Cisco IOS XE Release 3.2S	This command was modified. The *ipv6-address* argument was added.

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.

service pad

To enable all packet assembler/disassembler (PAD) commands and connections between PAD devices and access servers, use the **service pad** command in global configuration mode. To disable this service, use the **no** form of this command.

service pad [**cmns**] [**from-xot**] [**to-xot**]

no service pad [**cmns**] [**from-xot**] [**to-xot**]

Syntax Description

cmns	(Optional) Specifies sending and receiving PAD calls over CMNS.
from-xot	(Optional) Accepts XOT to PAD connections.
to-xot	(Optional) Allows outgoing PAD calls over XOT.

Command Default

All PAD commands and associated connections are enabled. PAD services over XOT or CMNS are not enabled.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
11.3	The **cmns** 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.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

The keywords **from-xot** and **to-xot** enable PAD calls to destinations that are not reachable over physical X.25 interfaces, but instead over TCP tunnels. This feature is known as PAD over XOT (X.25 over TCP).

Examples

If the **service pad** command is disabled, the **pad** EXEC command and all PAD related configurations, such as X.29, are unrecognized, as shown in the following example:

```
Router(config)# no service pad
Router(config)# x29 ?
% Unrecognized command
Router(config)# exit
Router# pad ?
% Unrecognized command
```

If the **service pad** command is enabled, the **pad** EXEC command and access to an X.29 configuration are granted as shown in the following example:

```
Router# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# service pad
Router(config)# x29 ?
access-list       Define an X.29 access list
inviteclear-time  Wait for response to X.29 Invite Clear message
profile           Create an X.3 profile
Router# pad ?
WORD   X121 address or name of a remote system
```

In the following example, PAD services over CMNS are enabled:

```
! Enable CMNS on a nonserial interface
interface ethernet0
 cmns enable
!
!Enable inbound and outbound PAD over CMNS service
service pad cmns
!
! Specify an X.25 route entry pointing to an interface's CMNS destination MAC address
x25 route ^2193330 interface Ethernet0 mac 00e0.b0e3.0d62

Router# show x25 vc

SVC 1,  State: D1,  Interface: Ethernet0
     Started 00:00:08, last input 00:00:08, output 00:00:08

     Line: 0   con 0    Location: console Host: 2193330
      connected to 2193330 PAD <--> CMNS Ethernet0 00e0.b0e3.0d62

     Window size input: 2, output: 2
     Packet size input: 128, output: 128
     PS: 2  PR: 3  ACK: 3  Remote PR: 2  RCNT: 0  RNR: no
     P/D state timeouts: 0  timer (secs): 0
     data bytes 54/19 packets 2/3 Resets 0/0 RNRs 0/0 REJs 0/0 INTs 0/0
```

Related Commands

Command	Description
cmns enable	Enables the CMNS on a nonserial interface.
show x25 vc	Displays information about active SVCs and PVCs.
x29 access-list	Limits access to the access server from certain X.25 hosts.
x29 profile	Creates a PAD profile script for use by the translate command.

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-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.
15.1(2)T	Support for IPv6 was added.

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.

service timestamps

To configure the system to apply a time stamp to debugging messages or system logging messages, use the **service timestamps** command in global configuration mode. To disable this service, use the **no** form of this command.

service timestamps [**debug | log**] [**uptime | datetime** [**msec**]] [**localtime**] [**show-timezone**] [**year**]

no service timestamps [**debug | log**]

Syntax Description

debug	(Optional) Indicates time-stamping for debugging messages.
log	(Optional) Indicates time-stamping for system logging messages.
uptime	(Optional) Specifies that the time stamp should consist of the time since the system was last rebooted. For example "4w6d" (time since last reboot is 4 weeks and 6 days). • This is the default time-stamp format for both debugging messages and logging messages. • The format for uptime varies depending on how much time has elapsed: – *HHHH*:*MM*:*SS* (*HHHH* hours: *MM* minutes: *SS* seconds) for the first 24 hours – *D*d*HH*h (*D* days *HH* hours) after the first day – *W*w*D*d (*W* weeks *D* days) after the first week
datetime	(Optional) Specifies that the time stamp should consist of the date and time. • The time-stamp format for **datetime** is MMM DD HH:MM:SS, where MMM is the month, DD is the date, HH is the hour (in 24-hour notation), MM is the minute, and SS is the second. • If the **datetime** keyword is specified, you can optionally add the **msec localtime**, **show-timezone**, or **year** keywords. • If the **service timestamps datetime** command is used without addtional keywords, time stamps will be shown using UTC, without the year, without milliseconds, and without a time zone name.
msec	(Optional) Includes milliseconds in the time stamp, in the format *HH*:*DD*:*MM*:*SS*.*mmm*, where *.mmm* is milliseconds
localtime	(Optional) Time stamp relative to the local time zone.
year	(Optional) Include the year in the date-time format.
show-timezone	(Optional) Include the time zone name in the time stamp. **Note** If the **localtime** keyword option is not used (or if the local time zone has not been configured using the **clock timezone** command), time will be displayed in Coordinated Universal Time (UTC).

Command Default Time stamps are applied to debug and logging messages.

Command Modes Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
11.3(5)	Service time stamps are enabled by default.
12.3(1)	The **year** keyword was added.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
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.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines Time stamps can be added to either debugging messages (**service timestamp debug**) or logging messages (**service timestamp log**) independently.

If the **service timestamps** command is specified with no arguments or keywords, the default is **service timestamps debug uptime**.

The **no service timestamps** command by itself disables time stamps for both debug and log messages.

The **uptime** form of the command adds time stamps (such as "2w3d") that indicating the time since the system was rebooted. The **datetime** form of the command adds time stamps (such as "Sep 5 2002 07:28:20") that indicate the date and time according to the system clock.

Entering the **service timestamps** {**debug** | **log**} command a second time will overwrite any previously configured **service timestamp** {**debug** | **log**} commands and associated options.

To set the local time zone, use the **clock timezone** *zone hours-offset* command in global configuration mode.

The time stamp will be preceeded by an asterisk or period if the time is potentially inaccurate. Table 49 describes the symbols that proceed the time stamp.

Table 49 Time-Stamping Symbols for syslog Messages

Symbol	Description	Example
(blank)	Time is authoritative: the software clock is in sync or has just been set manually	15:29:03.158 UTC Tue Feb 25 2003:
*	Time is not authoritative: the software clock has not been set, or is not in sync with configured Network Time Protocol (NTP) servers.	*15:29:03.158 UTC Tue Feb 25 2003:
.	Time is authoritative, but the NTP is not synchronized: the software clock was in sync, but has since lost contact with all configured NTP servers.	.15:29:03.158 UTC Tue Feb 25 2003:

Examples

In the following example, the router begins with time-stamping disabled. Then, the default time-stamping is enabled (uptime time stamps applied to debug output). Then, the default time-stamping for logging is enabled (uptime time stamps applied to logging output).

```
Router# show running-config | include time

no service timestamps debug uptime
no service timestamps log uptime

Router# config terminal
Router(config)# service timestamps
! issue the show running-config command in config mode using do
Router(config)# do show running-config | inc time
! shows that debug timestamping is enabled, log timestamping is disabled

service timestamps debug uptime
no service timestamps log uptime

! enable timestamps for logging messages
Router(config)# service timestamps log
Router(config)# do show run | inc time

service timestamps debug uptime
service timestamps log uptime

Router(config)# service sequence-numbers
Router(config)# end
000075: 5w0d: %SYS-5-CONFIG_I: Configured from console by console

! The following is a level 5 system logging message
! The leading number comes from the service sequence-numbers command.
! 4w6d indicates the timestamp of 4 weeks, 6 days

000075: 4w6d: %SYS-5-CONFIG_I: Configured from console by console
```

In the following example, the user enables time-stamping on logging messages using the current time and date in Coordinated Universal Time/Greenwich Mean Time (UTC/GMT), and enables the year to be shown.

```
Router(config)#
! The following line shows the timestamp with uptime (1 week 0 days)

1w0d: %SYS-5-CONFIG_I: Configured from console by console

Router(config)# service timestamps log datetime show-timezone year
Router(config)# end

! The following line shows the timestamp with datetime (11:13 PM March 22nd)

.Mar 22 2004 23:13:25 UTC: %SYS-5-CONFIG_I: Configured from console by console
```

The following example shows the change from UTC to local time:

```
Router# configure terminal

! Logging output can be quite long; first changing line width to show full
! logging message

Router(config)# line 0
Router(config-line)# width 180
Router(config-line)# logging synchronous
Router(config-line)# end
```

```
! Timestamping already enabled for logging messages; time shown in UTC.
Oct 13 23:20:05 UTC: %SYS-5-CONFIG_I: Configured from console by console

Router# show clock

23:20:53.919 UTC Wed Oct 13 2004

Router# configure terminal

Enter configuration commands, one per line.  End with the end command.

! Timezone set as Pacific Standard Time, with an 8 hour offset from UTC

Router(config)# clock timezone PST -8

Router(config)#

Oct 13 23:21:27 UTC: %SYS-6-CLOCKUPDATE:
System clock has been updated from 23:21:27 UTC Wed Oct 13 2004
to 15:21:27 PST Wed Oct 13 2004, configured from console by console.

Router(config)#
! Pacific Daylight Time (PDT) configured to start in April and end in October.
! Default offset is +1 hour.

Router(config)# clock summer-time PDT recurring first Sunday April 2:00 last Sunday
October 2:00

Router(config)#

! Time changed from 3:22 P.M. Pacific Standard Time (15:22 PST)
! to 4:22 P.M. Pacific Daylight (16:22 PDT)

Oct 13 23:22:09 UTC: %SYS-6-CLOCKUPDATE:
System clock has been updated from 15:22:09 PST Wed Oct 13 2004
to 16:22:09 PDT Wed Oct 13 2004, configured from console by console.

! Change the timestamp to show the local time and timezone.

Router(config)# service timestamps log datetime localtime show-timezone
Router(config)# end

Oct 13 16:23:19 PDT: %SYS-5-CONFIG_I: Configured from console by console

Router# show clock
16:23:58.747 PDT Wed Oct 13 2004
Router# config t
Enter configuration commands, one per line.  End with the end command.
Router(config)# service sequence-numbers
Router(config)# end
Router#
```

In the following example, the **service timestamps log datetime** command is used to change previously configured options for the date-time time stamp.

```
Router(config)# service timestamps log datetime localtime show-timezone

Router(config)# end

! The year is not displayed.

Oct 13 15:44:46 PDT: %SYS-5-CONFIG_I: Configured from console by console

Router# config t
```

```
Enter configuration commands, one per line.  End with the end command.
Router(config)# service timestamps log datetime show-timezone year
Router(config)# end

! note: because the localtime option was not specified again, that option is
! removed from the output, and time is displayed in UTC (the default)

Oct 13 2004 22:45:31 UTC: %SYS-5-CONFIG_I: Configured from console by console
```

Related Commands

Command	Description
clock set	Manually sets the system clock.
ntp	Controls access to the system's NTP services.
service sequence-numbers	Stamps system logging messages with a sequence number.

session protocol (dial peer)

To specify a session protocol for calls between local and remote routers using the packet network, use the **session protocol** command in dial-peer configuration mode. To reset to the default, use the **no** form of this command.

session protocol {**aal2-trunk** | **cisco** | **sipv2** | **smtp**}

no session protocol

Syntax Description

aal2-trunk	Dial peer uses ATM adaptation layer 2 (AAL2) nonswitched trunk session protocol.
cisco	Dial peer uses the proprietary Cisco VoIP session protocol.
sipv2	Dial peer uses the Internet Engineering Task Force (IETF) Session Initiation Protocol (SIP). Use this keyword with the SIP option.
smtp	Dial peer uses Simple Mail Transfer Protocol (SMTP) session protocol.

Command Default

No default behaviors or values

Command Modes

Dial-peer configuration (config-dial-peer)

Command History

Release	Modification
11.3(1)T	This command was introduced for VoIP peers on the Cisco 3600 series.
12.0(3)XG	This command was modified to support VoFR) dial peers.
12.0(4)XJ	This command was modified for store-and-forward fax on the Cisco AS5300.
12.1(1)XA	This command was implemented for VoATM dial peers on the Cisco MC3810. The **aal2-trunk** keyword was added.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T. The **sipv2** keyword was added.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.2(2)T	This command was implemented on the Cisco 7200 series.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and was implemented on the Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release. The **aal2-trunk** and **smtp** keywords are not supported on the Cisco 7200 series in this release.
12.2(11)T	This command is supported on the Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.

Usage Guidelines

The **cisco** keyword is applicable only to VoIP on the Cisco 1750, Cisco 1751, Cisco 3600 series, and Cisco 7200 series routers.

The **aal2-trunk** keyword is applicable only to VoATM on the Cisco 7200 series router.

This command applies to both on-ramp and off-ramp store-and-forward fax functions.

Examples

The following example shows that AAL2 trunking has been configured as the session protocol:

```
dial-peer voice 10 voatm
 session protocol aal2-trunk
```

The following example shows that Cisco session protocol has been configured as the session protocol:

```
dial-peer voice 20 voip
 session protocol cisco
```

The following example shows that a VoIP dial peer for SIP has been configured as the session protocol for VoIP call signaling:

```
dial-peer voice 102 voip
 session protocol sipv2
```

Related Commands

Command	Description
dial-peer voice	Enters dial-peer configuration mode and specifies the method of voice-related encapsulation.
session target (VoIP)	Configures a network-specific address for a dial peer.

session target (VoIP dial peer)

To designate a network-specific address to receive calls from a VoIP or VoIPv6 dial peer, use the **session target** command in dial peer configuration mode. To reset to the default, use the **no** form of this command.

Cisco 1751, Cisco 3725, Cisco 3745, and Cisco AS5300

session target {**dhcp** | **ipv4:***destination-address* | **ipv6:**[*destination-address*] | **dns:**[**s.** | **d.** | **e.** | **u.**] *hostname* | **enum:***table-num* | **loopback:rtp** | **ras** | **sip-server** | **registrar**} [**:***port*]

no session target

Cisco 2600 Series, Cisco 3600 Series, Cisco AS5350, Cisco AS5400, and Cisco AS5850

session target {**dhcp** | **ipv4:***destination-address* | **ipv6:**[*destination-address*] | **dns:**[**s.** | **d.** | **e.** | **u.**] *hostname* | **enum:***table-num* | **loopback:rtp** | **ras** | **settlement** *provider-number* | **sip-server** | **registrar**} [**:***port*]

no session target

Syntax Description

dhcp	Configures the router to obtain the session target via DHCP. **Note** The **dhcp** option can be made available only if the Session Initiation Protocol (SIP) is used as the session protocol. To enable SIP, use the **session protocol** (dial peer) command.
ipv4:*destination-address*	Configures the IP address of the dial peer to receive calls. The colon is required.
ipv6:[*destination-address*]	Configures the IPv6 address of the dial peer to receive calls. Square brackets must be entered around the IPv6 address. The colon is required.
dns:[s] *hostname*	Configures the host device housing the domain name system (DNS) server that resolves the name of the dial peer to receive calls. The colon is required. Use one of the following macros with this keyword when defining the session target for VoIP peers: • **s.**—(Optional) Source destination pattern is used as part of the domain name. • **d.**—(Optional) Destination number is used as part of the domain name. • **e.**—(Optional) Digits in the called number are reversed and periods are added between the digits of the called number. The resulting string is used as part of the domain name. • **u.**—(Optional) Unmatched portion of the destination pattern (such as a defined extension number) is used as part of the domain name. • *hostname*—String that contains the complete hostname to be associated with the target address; for example, serverA.example1.com.

enum:*table-num*	Configures ENUM search table number. Range is from 1 to 15. The colon is required.
loopback:rtp	Configures all voice data to loop back to the source. The colon is required.
ras	Configures the registration, admission, and status (RAS) signaling function protocol. A gatekeeper is consulted to translate the E.164 address into an IP address.
sip-server	Configures the global SIP server is the destination for calls from the dial peer.
:*port*	(Optional) Port number for the dial-peer address. The colon is required.
settlement *provider-number*	Configures the settlement server as the target to resolve the terminating gateway address. • The *provider-number* argument specifies the provider IP address.
registrar	Specifies to route the call to the registrar end point. • The **registrar** keyword is available only for SIP dial peers.

Command Default

No IP address or domain name is defined.

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 2600 series and Cisco 3600 series.
12.0(3)T	This command was modified. This command was implemented on the Cisco AS5300. The **ras** keyword was added.
12.0(4)XJ	This command was implemented for store-and-forward fax on the Cisco AS5300.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T. The **settlement** and **sip-server** keywords were added.
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 was not included in this release.
12.2(11)T	This command was implemented on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850. The **enum** keyword was added.
12.4(22)T	This command was modified. Support for IPv6 was added.
12.4(22)YB	This command was modified. The **dhcp** keyword was added.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
15.1(3)T	This command was modified. The **registrar** keyword was added.

Usage Guidelines

Use the **session target** command to specify a network-specific destination for a dial peer to receive calls from the current dial peer. You can select an option to define a network-specific address or domain name as a target, or you can select one of several methods to automatically determine the destination for calls from the current dial peer.

Use the **session target dns** command with or without the specified macros. Using the optional macros can reduce the number of VoIP dial-peer session targets that you must configure if you have groups of numbers associated with a particular router.

The **session target enum** command instructs the dial peer to use a table of translation rules to convert the dialed number identification service (DNIS) number into a number in E.164 format. This translated number is sent to a DNS server that contains a collection of URLs. These URLs identify each user as a destination for a call and may represent various access services, such as SIP, H.323, telephone, fax, e-mail, instant messaging, and personal web pages. Before assigning the session target to the dial peer, configure an ENUM match table with the translation rules using the **voice enum-match-table** command in global configuration mode. The table is identified in the **session target enum** command with the *table-num* argument.

Use the **session target loopback** command to test the voice transmission path of a call. The loopback point depends on the call origin.

Use the **session target dhcp** command to specify that the session target host is obtained via DHCP. The **dhcp** option can be made available only if the SIP is being used as the session protocol. To enable SIP, use the **session protocol** (dial peer) command.

In Cisco IOS Release 12.1(1)T the **session target** command configuration cannot combine the target of RAS with the **settle-call** command.

For the **session target settlement** *provider-number* command, when the VoIP dial peers are configured for a settlement server, the *provider-number* argument in the **session target** and **settle-call** commands should be identical.

Use the **session target sip-server** command to name the global SIP server interface as the destination for calls from the dial peer. You must first define the SIP server interface by using the **sip-server** command in SIP user-agent (UA) configuration mode. Then you can enter the **session target sip-server** option for each dial peer instead of having to enter the entire IP address for the SIP server interface under each dial peer.

After the SIP endpoints are registered with the SIP registrar in the hosted unified communications (UC), you can use the **session target registrar** command to route the call automatically to the registrar end point. You must configure the **session target** command on a dial pointing towards the end point.

Examples

The following example shows how to create a session target using DNS for a host named “voicerouter” in the domain example.com:

```
dial-peer voice 10 voip
 session target dns:voicerouter.example.com
```

The following example shows how to create a session target using DNS with the optional **u**. macro. In this example, the destination pattern ends with four periods (.) to allow for any four-digit extension that has the leading number 1310555. The optional **u**. macro directs the gateway to use the unmatched portion of the dialed number—in this case, the four-digit extension—to identify a dial peer. The domain is “example.com.”

```
dial-peer voice 10 voip
 destination-pattern 1310555....
 session target dns:$u$.example.com
```

The following example shows how to create a session target using DNS, with the optional **d**. macro. In this example, the destination pattern has been configured to 13105551111. The optional macro **d**. directs the gateway to use the destination pattern to identify a dial peer in the "example.com" domain.

```
dial-peer voice 10 voip
 destination-pattern 13105551111
 session target dns:$d$.example.com
```

The following example shows how to create a session target using DNS, with the optional **e**. macro. In this example, the destination pattern has been configured to 12345. The optional macro **e**. directs the gateway to do the following: reverse the digits in the destination pattern, add periods between the digits, and use this reverse-exploded destination pattern to identify the dial peer in the "example.com" domain.

```
dial-peer voice 10 voip
 destination-pattern 12345
 session target dns:$e$.example.com
```

The following example shows how to create a session target using an ENUM match table. It indicates that calls made using dial peer 101 should use the preferential order of rules in enum match table 3:

```
dial-peer voice 101 voip
 session target enum:3
```

The following example shows how to create a session target using DHCP:

```
dial-peer voice 1 voip
session protocol sipv2
voice-class sip outbound-proxy dhcp
session target dhcp
```

The following example shows how to create a session target using RAS:

```
dial-peer voice 11 voip
 destination-pattern 13105551111
 session target ras
```

The following example shows how to create a session target using settlement:

```
dial-peer voice 24 voip
 session target settlement:0
```

The following example shows how to create a session target using IPv6 for a host at 2001:10:10:10:10:10:10:230a:5090:

```
dial-peer voice 4 voip
destination-pattern 5000110011
session protocol sipv2
session target ipv6:[2001:0DB8:10:10:10:10:10:230a]:5090
codec g711ulaw
```

The following example shows how to configure Cisco Unified Border Element (UBE) to route a call to the registering end point:

```
dial-peer voice 4 voip
session target registrar
```

Related Commands

Command	Description
destination-pattern	Specifies either the prefix or the full E.164 telephone number (depending on the dial plan) to be used for a dial peer.
dial-peer voice	Enters dial peer configuration mode and specifies the method of voice-related encapsulation.
session protocol (dial peer)	Specifies a session protocol for calls between local and remote routers using the packet network dial peer configuration mode.
settle-call	Specifies that settlement is to be used for the specified dial peer, regardless of the session target type.
sip-server	Defines a network address for the SIP server interface.
voice enum-match-table	Initiates the ENUM match table definition.

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.
15.1(2)T	Support for IPv6 was added.

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.

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.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

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 default interface

To indicate where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination, use the **set default interface** command in route-map configuration mode. To delete an entry, use the **no** form of this command.

set default interface *type number* [*...type number*]

no set default interface *type number* [*...type number*]

Syntax Description

type	Interface type, used with the interface number, to which packets are output.
number	Interface number, used with the interface type, to which packets are output.

Command Default

This command is disabled by default.

Command Modes

Route-map configuration

Command History

Release	Modification
11.0	This command was introduced.
12.3(7)T	This command was updated for use in configuring IPv6 policy-based routing (PBR).
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)S.
12.2SX	This command is supported in the Cisco 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 modified. It was integrated into Cisco IOS XE Release 3.2S.

Usage Guidelines

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *type* and *number* arguments.

Use this command to provide certain users a different default route. If the Cisco IOS software has no explicit route for the destination, then it routes the packet to this interface. The first interface specified with the **set default interface** command that is up is used. The optionally specified interfaces are tried in turn.

Use the **ip policy route-map** interface configuration command, the **route-map** global configuration command, and the **match** and **set** route-map configuration commands to define the conditions for policy routing packets. The **ip policy route-map** command identifies a route map by name. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the match criteria—the conditions under which policy routing occurs. The **set** commands specify the set actions—the particular routing actions to perform if the criteria enforced by the **match** commands are met.

In PBR for IPv6, use the **ipv6 policy route-map** or **ipv6 local policy route-map** command with match and set route map configuration commands to define conditions for policy routing packets.

The set clauses can be used in conjunction with one another. They are evaluated in the following order:

1. **set ip next-hop**
2. **set interface**
3. **set ip default next-hop**
4. **set default interface**

Examples

In the following example, packets that have a Level 3 length of 3 to 50 bytes and for which the software has no explicit route to the destination are output to Ethernet interface 0:

```
interface serial 0
 ip policy route-map brighton
!
route-map brighton
 match length 3 50
 set default interface ethernet 0
```

Related Commands

Command	Description
ip policy route-map	Identifies a route map to use for policy routing on an interface.
ipv6 local policy route-map	Identifies a route map to use for local IPv6 PBR.
ipv6 policy route-map	Configures IPv6 PBR on an interface.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match ipv6 address	Specifies an IPv6 access list to use to match packets for PBR for IPv6.
match length	Bases policy routing on the Level 3 length of a packet.
route-map	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Indicates where to output packets that pass a match clause of route map for policy routing.
set ip default next-hop verify-availability	Indicates where to output packets that pass a match clause of a route map for policy routing and for which the Cisco IOS software has no explicit route to a destination.
set ipv6 default next-hop	Specifies an IPv6 default next hop to which matching packets will be forwarded.
set ip next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing.
set ipv6 next-hop (PBR)	Indicates where to output IPv6 packets that pass a match clause of a route map for policy routing.
set ipv6 precedence	Sets the precedence value in the IPv6 packet header.

set dscp

To mark a packet by setting the differentiated services code point (DSCP) value in the type of service (ToS) byte, use the **set dscp** command in QoS policy-map class configuration mode. To remove a previously set DSCP value, use the **no** form of this command.

set dscp {*dscp-value* | *from-field* [**table** *table-map-name*]}

no set dscp {*dscp-value* | *from-field* [**table** *table-map-name*]}

Syntax Description

dscp-value	A number that sets the DSCP value. The range is from 0 to 63. The following reserved keywords can be specified instead of numeric values: • **EF** (expedited forwarding) • **AF11** (assured forwarding class AF11) • **AF12** (assured forwarding class AF12)
from-field	Specific packet-marking category to be used to set the DSCP value of the packet. Packet-marking category keywords are as follows: • **cos** • **qos-group** **Note** If you are using a table map for mapping and converting packet-marking values, this establishes the "map from" packet-marking category.
table	(Optional) Indicates that the values set in a specified table map will be used to set the DSCP value. • This keyword is used in conjunction with the *from-field* argument.
table-map-name	(Optional) Name of the table map used to specify the DSCP value. The name can be a maximum of 64 alphanumeric characters. • This argument is used in conjunction with the **table** keyword.

Command Default

The DSCP value in the ToS byte is not set.

Command Modes

QoS policy-map class configuration (config-pmap-c)

Command History

Release	Modification
12.2(13)T	This command was introduced. It replaced the **set ip dscp** command.
12.0(28)S	This command was modified. Support for this command in IPv6 was added on the in Cisco IOS Release 12.0(28)S
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 and implemented on Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

Once the DSCP bit is set, other quality of service (QoS) features can then operate on the bit settings.

DSCP and Precedence Values Are Mutually Exclusive

The **set dscp** command cannot be used with the **set precedence** command to mark the *same* packet. The two values, DSCP and precedence, are mutually exclusive. A packet can have one value or the other, but not both.

Precedence Value and Queueing

The network gives priority (or some type of expedited handling) to marked traffic. Typically, you set the precedence value at the edge of the network (or administrative domain); data then is queued according to the precedence. Weighted fair queueing (WFQ) can speed up handling for high-precedence traffic at congestion points. Weighted Random Early Detection (WRED) ensures that high-precedence traffic has lower loss rates than other traffic during times of congestion.

Use of the "from-field" Packet-marking Category

If you are using this command as part of the Enhanced Packet Marking feature, it can specify the "from-field" packet-marking category to be used for mapping and setting the DSCP value. The "from-field" packet-marking categories are as follows:

- Class of service (CoS)
- QoS group

If you specify a "from-field" category but do not specify the **table** keyword and the applicable *table-map-nam*e argument, the default action will be to copy the value associated with the "from-field" category as the DSCP value. For instance, if you configure the **set dscp cos** command, the CoS value will be copied and used as the DSCP value.

Note The CoS field is a three-bit field, and the DSCP field is a six-bit field. If you configure the **set dscp cos** command, only the three bits of the CoS field will be used.

If you configure the **set dscp qos-group** command, the QoS group value will be copied and used as the DSCP value.

The valid value range for the DSCP is a number from 0 to 63. The valid value range for the QoS group is a number from 0 to 99. Therefore, when configuring the **set dscp qos-group** command, note the following points:

- If a QoS group value falls within both value ranges (for example, 44), the packet-marking value will be copied and the packets will be marked.
- If QoS group value exceeds the DSCP range (for example, 77), the packet-marking value will not be copied and the packet will not be marked. No action is taken.

Set DSCP Values in IPv6 Environments

When this command is used in IPv6 environments, the default match occurs on both IP and IPv6 packets. However, the actual packets set by this function are only those that meet the match criteria of the class map containing this function.

Set DSCP Values for IPv6 Packets Only

To set DSCP values for IPv6 values only, you must also use the **match protocol ipv6** command. Without that command, the precedence match defaults to match both IPv4 and IPv6 packets.

Set DSCP Values for IPv4 Packets Only

To set DSCP values for IPv4 values only, you must use the appropriate **match ip** command. Without this command, the class map may match both IPv6 and IPv4 packets, depending on the other match criteria, and the DSCP values may act upon both types of packets.

Examples

Packet-marking Values and Table Map

In the following example, the policy map called "policy1" is created to use the packet-marking values defined in a table map called "table-map1". The table map was created earlier with the **table-map** (value mapping) command. For more information about the **table-map** (value mapping) command, see the **table-map** (value mapping) command page.

In this example, the DSCP value will be set according to the CoS value defined in the table map called "table-map1".

```
Router(config)# policy-map policy1
Router(config-pmap)# class class-default
Router(config-pmap-c)# set dscp cos table table-map1
Router(config-pmap-c)# end
```

The **set dscp** command is applied when you create a service policy in QoS policy-map configuration mode. This service policy is not yet attached to an interface. For information on attaching a service policy to an interface, see the "Modular Quality of Service Command-Line Interface" section of the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Related Commands

Command	Description
match ip dscp	Identifies one or more DSCP, AF, and CS values as a match criterion
match protocol	Configures the match criteria for a class map on the basis of the specified protocol.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
service-policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.
set cos	Sets the Layer 2 CoS value of an outgoing packet.
set precedence	Sets the precedence value in the packet header.
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 class	Displays the configuration for the specified class of the specified policy map.
show policy-map interface	Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface.
show table-map	Displays the configuration of a specified table map or all table maps.
table-map (value mapping)	Creates and configures a mapping table for mapping and converting one packet-marking value to another.

set extcommunity

To set Border Gateway Protocol (BGP) extended community attributes, use the **set extcommunity** command in route-map configuration mode. To delete the entry, use the **no** form of this command.

set extcommunity {**rt** [*extended-community-value*] [**additive**] | **soo** [*extended-community-value*]}

no set extcommunity

Syntax Description

rt	Specifies the route target (RT) extended community attribute.
soo	Specifies the site of origin (SOO) extended community attribute.
extended-community-value	(Optional) Specifies the value to be set. The value can be one of the following combinations: • *autonomous-system-number*:*network-number* • *ip-address*:*network-number* • *ipv6-address*:*network-number* The colon is used to separate the autonomous system number and network number, the IP address and network number, or the IPv6 address and network number. • In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, 4-byte autonomous system numbers are supported in the range from 65536 to 4294967295 in asplain notation and in the range from 1.0 to 65535.65535 in asdot notation. • In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, 4-byte autonomous system numbers are supported in the range from 1.0 to 65535.65535 in asdot notation only. For more details about autonomous system number formats, see the **router bgp** command.
additive	(Optional) Adds a route target to the existing route target list without replacing any existing route targets.

Command Default

Specifying new route targets with the **rt** keyword replaces existing route targets by default, unless the **additive** keyword is used. The use of the **additive** keyword adds the new route target to the existing route target list but does not replace any existing route targets.

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
12.1	This command was introduced.
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.

Release	Modification
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	Support for IPv6 was added. and this command was integrated into Cisco IOS Release 12.2(33)SB.
12.0(32)S12	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(24)T	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.3	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SXI1	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
12.2(33)SRE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.

Usage Guidelines

Extended community attributes are used to configure, filter, and identify routes for virtual routing and forwarding instances (VRFs) and Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs).

The **set extcommunity** command is used to configure set clauses that use extended community attributes in route maps. All of the standard rules of match and set clauses apply to the configuration of extended community attributes.

The route target (RT) extended community attribute is configured with the **rt** keyword. This attribute is used to identify a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that are used for routing traffic that is received from corresponding sites.

The site of origin (SOO) extended community attribute is configured with the **soo** keyword. This attribute uniquely identifies the site from which the Provider Edge (PE) router learned the route. All routes learned from a particular site must be assigned the same SOO extended community attribute, whether a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents routing loops from occurring when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO can be applied to routes that are learned from VRFs. The SOO should not be configured for stub sites or sites that are not multihomed.

In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, the Cisco implementation of 4-byte autonomous system numbers uses asplain—65538 for example—as the default regular expression match and output display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain format and the asdot format as described in RFC 5396. To change the default regular expression

match and output display of 4-byte autonomous system numbers to asdot format, use the **bgp asnotation dot** command followed by the **clear ip bgp *** command to perform a hard reset of all current BGP sessions.

In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, the Cisco implementation of 4-byte autonomous system numbers uses asdot—1.2 for example—as the only configuration format, regular expression match, and output display, with no asplain support.

Examples

The following example sets the route target to extended community attribute 100:2 for routes that are permitted by the route map:

```
Router(config)# access-list 2 permit 192.168.78.0 255.255.255.0
Router(config)# route-map MAP_NAME permit 10
Router(config-route-map)# match ip-address 2
Router(config-route-map)# set extcommunity rt 100:2
```

The following example sets the route target to extended community attribute 100:3 for routes that are permitted by the route map. The use of the **additive** keyword adds route target 100:3 to the existing route target list but does not replace any existing route targets.

```
Router(config)# access-list 3 permit 192.168.79.0 255.255.255.0
Router(config)# route-map MAP_NAME permit 10
Router(config-route-map)# match ip-address 3
Router(config-route-map)# set extcommunity rt 100:3 additive
```

Note Configuring route targets with the **set extcommunity** command will replace existing route targets, unless the **additive** keyword is used.

The following example sets the site of origin to extended community attribute 100:4 for routes that are permitted by the route map:

```
Router(config)# access-list 4 permit 192.168.80.0 255.255.255.0
Router(config)# route-map MAP_NAME permit 10
Router(config-route-map)# match ip-address 4
Router(config-route-map)# set extcommunity soo 100:4
```

In IPv6, the following example sets the SoO to extended community attribute 100:28 for routes that are permitted by the route map:

```
(config)# router bgp 100
(config-router)# address-family ipv6 vrf red
(config-router-af)# neighbor 8008::72a route-map setsoo in
(config-router-af)# exit
(config-router)# route-map setsoo permit 10
(config-router)# set extcommnunity soo 100:28
```

The following example available in Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, shows how to create a VRF with a route-target that uses a 4-byte autonomous system number, 65537 in asplain format, and how to set the route-target to extended community value 65537:100 for routes that are permitted by the route map.

```
Router(config)# ip vrf vpn_red
Router(config-vrf)# rd 64500:100
Router(config-vrf)# route-target both 65537:100
Router(config-vrf)# exit
Router(config)# route-map rt_map permit 10
Router(config-route-map)# set extcommunity rt 65537:100
Router(config-route-map)# end
```

The following example available in Cisco IOS Release 12.0(32)SY8, 12.0(32)S12, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, 12.4(24)T, Cisco IOS XE Release 2.3, and later releases, shows how to create a VRF with a route-target that uses a 4-byte autonomous system number, 1.1 in asdot format, and how to set the SoO to extended community attribute 1.1:100 for routes that are permitted by the route map.

```
Router(config)# ip vrf vpn_red
Router(config-vrf)# rd 64500:100
Router(config-vrf)# route-target both 1.1:100
Router(config-vrf)# exit
Router(config)# route-map soo_map permit 10
Router(config-route-map)# set extcommunity soo 1.1:100
Router(config-route-map)# end
```

Related Commands

Command	Description
bgp asnotation dot	Changes the default display and the regular expression match format of BGP 4-byte autonomous system numbers from asplain (decimal values) to dot notation.
ip extcommunity-list	Creates an extended community list and controls access to it.
match extcommunity	Matches a BGP VPN extended community list.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
router bgp	Configures the BGP routing process.
route-target	Creates a route target extended community for a VRF.
show ip extcommunity-list	Displays routes that are permitted by the extended community list.
show route-map	Displays all route maps configured or only the one specified.

set interface

To indicate where to forward packets that pass a match clause of a route map for policy routing, use the **set interface** command in route-map configuration mode. To delete an entry, use the **no** form of this command.

set interface *type number* [*...type number*]

no set interface *type number* [*...type number*]

Syntax Description

type	Interface type, used with the interface number, to which packets are forwarded.
number	Interface number, used with the interface type, to which packets are forwarded.

Command Default

Packets that pass a match clause are not forwarded to an interface.

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
11.0	This command was introduced.
12.3(7)T	This command was updated for use in configuring IPv6 policy-based routing (PBR).
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB, and hardware switching support was introduced for the Cisco 7600 series platform.
12.2SX	This command was integrated into the Cisco 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 modified. It was integrated into Cisco IOS XE Release 3.2S.

Usage Guidelines

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *type* and *number* arguments.

Use the **ip policy route-map** interface configuration command, the **route-map** global configuration command, and the **match** and **set** route-map configuration commands to define the conditions for policy-routing packets. The **ip policy route-map** command identifies a route map by name. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*—the conditions under which policy routing occurs. The **set** commands specify the *set actions*—the particular routing actions to perform if the criteria enforced by the **match** commands are met.

In PBR for IPv6, use the **ipv6 policy route-map** or **ipv6 local policy route-map** command with **match** and **set** route-map configuration commands to define conditions for policy-routing packets.

If the first interface specified with the **set interface** command is down, the optionally specified interfaces are tried in turn.

The **set** clauses can be used in conjunction with one another. They are evaluated in the following order:

1. **set ip next-hop**
2. **set interface**
3. **set ip default next-hop**
4. **set default interface**

A useful next hop implies an interface. As soon as a next hop and an interface are found, the packet is routed.

Specifying the **set interface null 0** command is a way to write a policy that the packet be dropped and an "unreachable" message be generated. In Cisco IOS Release 12.4(15)T and later releases, the packets are dropped; however, the "unreachable" messages are generated only when CEF is disabled.

In Cisco IOS Release 12.2(33)SRB and later releases, hardware switching support was introduced for PBR packets sent over a traffic engineering (TE) tunnel interface on a Cisco 7600 series router. When a TE tunnel interface is configured using the **set interface** command in a policy, the packets are processed in hardware. In previous releases, PBR packets sent over TE tunnels are fast switched by Route Processor software.

Examples

In the following example, packets with a Level 3 length of 3 to 50 bytes are forwarded to Ethernet interface 0:

```
interface serial 0
 ip policy route-map testing
!
route-map testing
 match length 3 50
 set interface ethernet 0
```

In the following example for IPv6, packets with a Level 3 length of 3 to 50 bytes are forwarded to Ethernet interface 0:

```
interface serial 0
 ipv6 policy route-map testing
!
route-map testing
 match length 3 50
 set interface ethernet 0
```

In the following example, a TE tunnel interface is configured on a Cisco 7600 series router using the **set interface** command in a policy, and the packets are processed in hardware, instead of being fast switched by Route Processor software. This example can be used only with a Cisco IOS Release 12.2(33)SRB, or later release, image.

```
interface Tunnel101
 description FRR-Primary-Tunnel
 ip unnumbered Loopback0
 tunnel destination 172.17.2.2
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng path-option 1 explicit name p1
!
access-list 101 permit ip 10.100.0.0 0.255.255.255 any
!
route-map test permit 10
 match ip address 101
 set interface Tunnel101
!
```

```
interface GigabitEthernet9/5
 description TO_CE_C1A_FastEther-5/5
 ip address 192.168.5.1 255.255.255.0
 ip policy route-map test
 no keepalive
```

Related Commands

Command	Description
ip policy route-map	Identifies a route map to use for policy routing on an interface.
ipv6 local policy route-map	Configures PBR for IPv6 for originated packets.
ipv6 policy route-map	Configures IPv6 PBR on an interface.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match ipv6 address	Specifies an IPv6 access list to use to match packets for PBR for IPv6.
match length	Bases policy routing on the Level 3 length of a packet.
route-map	Defines the conditions for redistributing routes from one routing protocol into another or enables policy routing.
set default interface	Indicates where to forward packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set ip default next-hop verify-availability	Indicates where to forward packets that pass a match clause of a route map for policy routing and for which the Cisco IOS software has no explicit route to a destination.
set ip next-hop	Indicates where to forward packets that pass a match clause of a route map for policy routing.
set ipv6 default next-hop	Specifies an IPv6 default next hop to which matching packets will be forwarded.
set ipv6 next-hop (PBR)	Indicates where to output IPv6 packets that pass a match clause of a route map for policy routing.
set ipv6 precedence	Sets the precedence value in the IPv6 packet header.

set ip next-hop

To indicate where to output packets that pass a match clause of a route map for policy routing, use the **set ip next-hop** command in route-map configuration mode. To delete an entry, use the **no** form of this command.

set ip next-hop {*ip-address* [*...ip-address*] | **dynamic dhcp** | **encapsulate l3vpn** *profile name* | **peer-address** | **recursive [global** | **vrf** *vrf name***]** *ip-address* | **verify-availability** [*ip-address sequence* **track** *track object number*}

no set ip next-hop *ip-address* [*...ip-address*]

Syntax Description

ip-address	IP address of the next hop to which packets are output. It must be the address of an adjacent router.
dynamic dhcp	Sets dynamically the DHCP next hop.
encapsulate l3vpn	Sets the encapsulation profile for VPN nexthop.
profile name	The L3VPN encapsulation profile name.
peer-address	Sets the next hop to be the BGP peering address.
recursive *ip-address*	Sets the IP address of the recursive next-hop router. **Note** The next-hop IP address must be assigned separately from the recursive next-hop IP address.
global	Sets the global routing table.
vrf *vrf name*	Sets the VRF.
verify-availability	Verifies if the nexthop is reachable.
sequence	(Optional) The sequence to insert into next-hop list. The range is from 1 to 65535.
track	(Optional) Sets the next hop depending on the state of a tracked object.
track object number	(Optional) The tracked object number. The range is from 1 to 500.

Command Default

Packets are forwarded to the next hop router in the routing table.

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
11.0	This command was introduced.
12.0(28)S	The **recursive** keyword was added.
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 12.2(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.
Cisco IOS XE Release 2.2	In Cisco IOS XE Release 2.2 this command was introduced on the Cisco ASR 1000 Series Routers.
12.2(33)SRE	This command was modified. The **encapsulate l3vpn** keyword was added.

Usage Guidelines

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *ip-address* argument.

Use the **ip policy route-map** interface configuration command, the **route-map** global configuration command, and the **match** and **set** route-map configuration commands to define the conditions for policy routing packets. The **ip policy route-map** command identifies a route map by name. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*—the conditions under which policy routing occurs. The **set** commands specify the *set actions*—the particular routing actions to perform if the criteria enforced by the **match** commands are met.

If the interface associated with the first next hop specified with the **set ip next-hop** command is down, the optionally specified IP addresses are tried in turn.

The set clauses can be used in conjunction with one another. They are evaluated in the following order:

1. **set ip next-hop**
2. **set interface**
3. **set ip default next-hop**
4. **set default interface**

Note The **set ip next-hop** and **set ip default next-hop** are similar commands but have a different order of operations. Configuring the **set ip next-hop** command causes the system to use policy routing first and then use the routing table. Configuring the **set ip default next-hop** command causes the system to use the routing table first and then policy route the specified next hop.

Examples

In the following example, packets with a Level 3 length of 3 to 50 bytes are output to the router at IP address 10.14.2.2:

```
interface serial 0
 ip policy route-map thataway
!
route-map thataway
 match length 3 50
 set ip next-hop 10.14.2.2
```

In the following example, the IP address of 10.3.3.3 is set as the recursive next-hop address:

```
route-map map_recurse
 set ip next-hop recursive 10.3.3.3
```

Related Commands

Command	Description
ip policy route-map	Identifies a route map to use for policy routing on an interface.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match length	Bases policy routing on the Level 3 length of a packet.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Indicates where to output packets that pass a match clause of route map for policy routing.
set ip default next-hop verify-availability	Indicates where to output packets that pass a match clause of a route map for policy routing and for which the Cisco IOS software has no explicit route to a destination.

set ipv6 default next-hop

To specify an IPv6 default next hop to which matching packets will be forwarded, use the **set ipv6 default next-hop** command in route-map configuration mode. To delete the default next hop, use the **no** form of this command.

set ipv6 default next-hop *global-ipv6-address* [*global-ipv6-address*...]

no set ipv6 default next-hop *global-ipv6-address* [*global-ipv6-address*...]

Syntax Description

global-ipv6-address	IPv6 global address of the next hop to which packets are output. The next-hop router must be an adjacent router. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

Command Default

This command is disabled by default.

Command Modes

Route-map configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)S.
12.2(33)SXI4	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SXI4.
Cisco IOS XE Release 3.2S	This command was modified. It was integrated into Cisco IOS XE Release 3.2S.

Usage Guidelines

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *global-ipv6-address* argument.

Use the **set ipv6 default next-hop** command in policy-based routing PBR for IPv6 to specify an IPv6 next-hop address to which a packet will be policy routed when the router has no route in the IPv6 routing table or the packets match the default route. The IPv6 next-hop address must be adjacent to the router; that is, reachable by using a directly connected IPv6 route in the IPv6 routing table. The IPv6 next-hop address also must be a global IPv6 address. An IPv6 link-local address cannot be used because use of an IPv6 link-local address requires interface context.

If the software has no explicit route for the destination in the packet, then it routes the packet to the next hop as specified by the **set ipv6 default next-hop** command. The optional specified IPv6 addresses are tried in turn.

Use the **ipv6 policy route-map** command, the **route-map** command, and the **match** and **set route-map** commands to define the conditions for PBR packets. The **ipv6 policy route-map** command identifies a route map by name. Each **route-map** command has a list of **match** and **set** commands associated with

it. The **match** commands specify the match criteria, which are the conditions under which PBR occurs. The **set** commands specify the set actions, which are the particular routing actions to perform if the criteria enforced by the match commands are met.

The set clauses can be used in conjunction with one another. They are evaluated in the following order:

1. **set ipv6 next-hop**
2. **set interface**
3. **set ipv6 default next-hop**
4. **set default interface**

Note The **set ipv6 next-hop** and **set ipv6 default next-hop** are similar commands. The **set ipv6 next-hop** command is used to policy route packets for which the router has a route in the IPv6 routing table. The **set ipv6 default next-hop** command is used to policy route packets for which the router does not have a route in the IPv6 routing table (or the packets match the default route).

Examples

The following example sets the next hop to which the packet will be routed:

```
ipv6 access-list match-dst-1
  permit ipv6 any 2001:0678::/32 any

route-map pbr-v6-default
  match ipv6 address match-dst-1
  set ipv6 default next-hop 2001:0089::1234
```

Related Commands

Command	Description
ipv6 local policy route-map	Identifies a route map to use for local IPv6 PBR.
ipv6 policy route-map	Configures IPv6 policy-based routing (PBR) on an interface.
match ipv6 address	Specifies an IPv6 access list to use to match packets for PBR for IPv6.
match length	Bases policy routing on the Level 3 length of a packet.
route-map (IP)	Define the conditions for redistributing routes from one routing protocol into another, or to enable policy routing.
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Indicates where to output packets that pass a match clause of a route map for policy routing.
set ipv6 next-hop (PBR)	Indicates where to output IPv6 packets that pass a match clause of a route map for policy routing.
set ipv6 precedence	Sets the precedence value in the IPv6 packet header.

set ipv6 next-hop (BGP)

To indicate where to output IPv6 packets that pass a match clause of a route map for policy routing, use the **set ipv6 next-hop** command in route-map configuration mode. To delete an entry, use the **no** form of this command.

set ipv6 next-hop {*ipv6-address* [*link-local-address*] | **encapsulate l3vpn** *profile name* | **peer-address**}

no set ipv6 next-hop {*ipv6-address* [*link-local-address*] | **encapsulate l3vpn** *profile name* | **peer-address**}

Syntax Description

ipv6-address	IPv6 global address of the next hop to which packets are output. It need not be an adjacent router. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
link-local-address	(Optional) IPv6 link-local address of the next hop to which packets are output. It must be an adjacent router. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
encapsulate l3vpn	Sets the encapsulation profile for VPN nexthop.
profile name	Name of the Layer 3 encapsulation profile.
peer-address	(Optional) Sets the next hop to be the BGP peering address.

Command Default

IPv6 packets are forwarded to the next hop router in the routing table.

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
12.2(4)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 Release 12.2(14)S.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
12.2(33)SRE	This command was modified. The **encapsulate l3vpn** keyword was added.

Usage Guidelines

The **set ipv6 next-hop** command is similar to the **set ip next-hop** command, except that it is IPv6-specific.

The **set** commands specify the *set actions*—the particular routing actions to perform if the criteria enforced by the **match** commands are met.

When the **set ipv6 next-hop** command is used with the **peer-address** keyword in an inbound route map of a BGP peer, the next hop of the received matching routes will be set to be the neighbor peering address, overriding any third-party next hops. So the same route map can be applied to multiple BGP peers to override third-party next hops.

When the **set ipv6 next-hop** command is used with the **peer-address** keyword in an outbound route map of a BGP peer, the next hop of the advertised matching routes will be set to be the peering address of the local router, thus disabling the next hop calculation. The **set ipv6 next-hop** command has finer granularity than the per-neighbor **neighbor next-hop-self** command, because you can set the next hop for some routes, but not others. The **neighbor next-hop-self** command sets the next hop for all routes sent to that neighbor.

The set clauses can be used in conjunction with one another. They are evaluated in the following order:

1. **set ipv6 next-hop**
2. **set interface**
3. **set ipv6 default next-hop**
4. **set default interface**

Examples

The following example configures the IPv6 multiprotocol BGP peer FE80::250:BFF:FE0E:A471 and sets the route map named nh6 to include the IPv6 next hop global addresses of Fast Ethernet interface 0 of the neighbor in BGP updates. The IPv6 next hop link-local address can be sent to the neighbor by the nh6 route map or from the interface specified by the **neighbor update-source** router configuration command.

```
router bgp 170
 neighbor FE80::250:BFF:FE0E:A471 remote-as 150
 neighbor FE80::250:BFF:FE0E:A471 update-source fastether 0

address-family ipv6
  neighbor FE80::250:BFF:FE0E:A471 activate
  neighbor FE80::250:BFF:FE0E:A471 route-map nh6 out

route-map nh6
 set ipv6 next-hop 3FFE:506::1
```

Note If you specify only the global IPv6 next hop address (the *ipv6-address* argument) with the **set ipv6 next-hop** command after specifying the neighbor interface (the *interface-type* argument) with the **neighbor update-source** command, the link-local address of the neighbor interface is included as the next hop in the BGP updates. Therefore, only one route map that sets the global IPv6 next hop address in BGP updates is required for multiple BGP peers that use link-local addresses.

Related Commands

Command	Description
ip policy route-map	Identifies a route map to use for policy routing on an interface.
match ipv6 address	Distributes IPv6 routes that have a prefix permitted by a prefix list.
match ipv6 next-hop	Distributes IPv6 routes that have a next hop prefix permitted by a prefix list.
match ipv6 route-source	Distributes IPv6 routes that have been advertised by routers at an address specified by a prefix list.

Command	Description
neighbor next-hop-self	Disables next-hop processing of BGP updates on the router.
neighbor update-source	Specifies that the Cisco IOS software allow BGP sessions to use any operational interface for TCP connections
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.

set ipv6 next-hop (PBR)

To indicate where to output IPv6 packets that pass a match clause of a route map for policy-based routing (PBR), use the **set ipv6 next-hop** command in route-map configuration mode. To delete an entry, use the **no** form of this command.

set ipv6 next-hop *global-ipv6-address* [*global-ipv6-address...*]

no set ipv6 next-hop *global-ipv6-address* [*global-ipv6-address...*]

Syntax Description

global-ipv6-address	IPv6 global address of the next hop to which packets are output. The next-hop router must be an adjacent router. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

Command Default

This command is not enabled.

Command Modes

Route-map configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)S.
12.2(33)SXI4	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SXI4.
Cisco IOS XE Release 3.2S	This command was modified. It was integrated into Cisco IOS XE Release 3.2S.

Usage Guidelines

The **set ipv6 next-hop** command is similar to the **set ip next-hop** command, except that it is IPv6-specific.

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *global-ipv6-address* argument. A global IPv6 address must be specified. An IPv6 link-local address cannot be used because use of an IPv6 link-local address requires interface context.

The *global-ipv6-address* argument must specify an address that is installed in the IPv6 Routing Information Base (RIB) and is directly connected. A directly connected address is an address that is covered by an IPv6 prefix configured on an interface or an address covered by an IPv6 prefix specified on a directly connected static route.

Examples

The following example sets the next hop to which the packet will be routed:

```
ipv6 access-list match-dst-1
  permit ipv6 any 2001:0678::/32 any
```

```
route-map pbr-v6-default
  match ipv6 address match-dst-1
  set ipv6 next-hop 2001:0089::1234
```

Related Commands

Command	Description
ipv6 local policy route-map	Identifies a route map to use for local IPv6 PBR.
ipv6 policy route-map	Configures IPv6 PBR on an interface.
match ipv6 address	Specifies an IPv6 access list to use to match packets for PBR for IPv6.
match length	Bases policy routing on the Level 3 length of a packet.
route-map (IP)	Define the conditions for redistributing routes from one routing protocol into another, or to enable policy routing.
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Indicates where to output packets that pass a match clause of a route map for policy routing.
set ipv6 default next-hop	Specifies an IPv6 default next hop to which matching packets will be forwarded.
set ipv6 precedence	Sets the precedence value in the IPv6 packet header.

set ipv6 precedence

To set the precedence value in the IPv6 packet header, use the **set ipv6 precedence** command in route-map configuration mode. To remove the precedence value, use the **no** form of this command.

set ipv6 precedence *precedence-value*

no set ipv6 precedence *precedence-value*

Syntax Description

precedence-value	A number from 0 to 7 that sets the precedence bit in the packet header.

Command Default

This command has no default behavior.

Command Modes

Route-map configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)S.
12.2(33)SXI4	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SXI4.
Cisco IOS XE Release 3.2S	This command was modified. It was integrated into Cisco IOS XE Release 3.2S.

Usage Guidelines

The way the network gives priority (or some type of expedited handling) to the marked traffic is through the application of weighted fair queueing (WFQ) or weighted random early detection (WRED) at points downstream in the network. Typically, you would set IPv6 precedence at the edge of the network (or administrative domain) and have queueing act on it thereafter. WFQ can speed up handling for high precedence traffic at congestion points. WRED ensures that high precedence traffic has lower loss rates than other traffic during times of congestion.

The mapping from keywords such as routine and priority to a precedence value is useful only in some instances. That is, the use of the precedence bit is evolving. You can define the meaning of a precedence value by enabling other features that use the value. In the case of Cisco high-end Internet quality of service (QoS), IPv6 precedences can be used to establish classes of service that do not necessarily correspond numerically to better or worse handling in the network. For example, IPv6 precedence 2 can be given 90 percent of the bandwidth on output links in the network, and IPv6 precedence 6 can be given 5 percent using the distributed weight fair queueing (DWFQ) implementation on the Versatile Interface Processors (VIPs).

Use the **route-map** global configuration command with **match** and **set** route-map configuration commands to define the conditions for redistributing routes from one routing protocol into another, or for policy routing. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the match criteria—the conditions under which redistribution or policy

routing is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular redistribution or policy routing actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **set route-map** configuration commands specify the redistribution set actions to be performed when all the match criteria of a route map are met. When all match criteria are met, all set actions are performed.

Examples

The following example sets the IPv6 precedence value to 5 for packets that pass the route map match:

```
interface serial 0
 ipv6 policy route-map texas
!
route-map cisco1
 match length 68 128
 set ipv6 precedence 5
```

Related Commands

Command	Description
ipv6 local policy route-map	Identifies a route map to use for local IPv6 PBR.
ipv6 policy route-map	Configures IPv6 PBR on an interface.
match ipv6 address	Specifies an IPv6 access list to use to match packets for PBR for IPv6.
match length	Bases policy routing on the Level 3 length of a packet.
route-map (IP)	Define the conditions for redistributing routes from one routing protocol into another, or to enable policy routing.
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Indicates where to output packets that pass a match clause of a route map for policy routing.
set ipv6 default next-hop	Specifies an IPv6 default next hop to which matching packets will be forwarded.
set ipv6 next-hop	Indicates where to output IPv6 packets that pass a match clause of a route map for policy routing.
set ipv6 precedence	Sets the precedence value in the IPv6 packet header.

set mpls-label

To enable a route to be distributed with a Multiprotocol Label Switching (MPLS) label if the route matches the conditions specified in the route map, use the **set mpls-label** command in route-map configuration mode. To disable this function, use the **no** form of this command.

set mpls-label

no set mpls-label

Syntax Description

This command has no arguments or keywords.

Command Default

No route with an MPLS label is distributed.

Command Modes

Route-map configuration

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(11)S	This command was integrated into Cisco IOS Release 12.2(11)S.
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.
12.2(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)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

This command can be used only with the **neighbor route-map out** command to manage outbound route maps for a Border Gateway Protocol (BGP) session.

Use the **route-map** global configuration command with **match** and **set route-map** commands to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the match criteria—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

Examples

The following example shows how to create a route map that enables the route to be distributed with a label if the IP address of the route matches an IP address in ACL1:

```
Router(config-router)# route-map incoming permit 10
Router(config-route-map)# match ip address 1
```

```
Router(config-route-map)# set mpls-label
```

Related Commands

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.
match ipv6 address	Distributes IPv6 routes that have a prefix permitted by a prefix list or specifies an IPv6 access list to use to match packets for PBR for IPv6.
match mpls-label	Redistributes routes that contain MPLS labels and match the conditions specified in the route map.
neighbor route-map out	Manage outbound route maps for a BGP session.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.

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 precedence

To set the precedence value in the packet header, use the **set precedence** command in policy-map class configuration mode. To remove the precedence value, use the **no** form of this command.

Supported Platforms Other Than Cisco 10000 Series Routers

set precedence {*precedence-value* | *from-field* [**table** *table-map-name*]}

no set precedence {*precedence-value* | *from-field* [**table** *table-map-name*]}

Cisco 10000 Series Routers

set precedence *precedence-value*

no set precedence *precedence-value*

Syntax Description

precedence-value	A number from 0 to 7 that sets the precedence bit in the packet header.
from-field	Specific packet-marking category to be used to set the precedence value of the packet. If you are using a table map for mapping and converting packet-marking values, this argument value establishes the "map from" packet-marking category. Packet-marking category keywords are as follows: • **cos** • **qos-group**
table	(Optional) Indicates that the values set in a specified table map will be used to set the precedence value.
table-map-name	(Optional) Name of the table map used to specify a precedence value based on the class of service (CoS) value. The name can be a maximum of 64 alphanumeric characters.

Command Default

This command is disabled.

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.2(13)T	This command was introduced. This command replaces the **set ip precedence** command.
12.0(28)S	Support for this command in IPv6 was added in Cisco IOS Release 12.0(28)S on the Cisco 12000 series Internet routers.
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 and implemented on the Cisco 10000 series router.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

Command Compatibility

If a router is loaded with an image from this version (that is, Cisco IOS Release 12.2(13)T) that contained an old configuration, the **set ip precedence** command is still recognized. However, the **set precedence** command will be used in place of the **set ip precedence** command.

The **set precedence** command cannot be used with the **set dscp** command to mark the *same* packet. The two values, DSCP and precedence, are mutually exclusive. A packet can be one value or the other, but not both.

Bit Settings

Once the precedence bits are set, other quality of service (QoS) features such as weighted fair queueing (WFQ) and Weighted Random Early Detection (WRED) then operate on the bit settings.

Precedence Value

The network gives priority (or some type of expedited handling) to marked traffic through the application of WFQ or WRED at points downstream in the network. Typically, you set the precedence value at the edge of the network (or administrative domain); data then is queued according to the specified precedence. WFQ can speed up handling for certain precedence traffic at congestion points. WRED can ensure that certain precedence traffic has lower loss rates than other traffic during times of congestion.

The **set precedence** command cannot be used with the **set dscp** command to mark the *same* packet. The two values, differentiated services code point (DSCP) and precedence, are mutually exclusive. A packet can have one value or the other, but not both.

Using This Command with the Enhanced Packet Marking Feature

If you are using this command as part of the Enhanced Packet Marking feature, you can use this command to specify the "from-field" packet-marking category to be used for mapping and setting the precedence value. The "from-field" packet-marking categories are as follows:

- CoS
- QoS group

If you specify a "from-field" category but do not specify the **table** keyword and the applicable *table-map-nam*e argument, the default action will be to copy the value associated with the "from-field" category as the precedence value. For instance, if you configure the **set precedence cos** command, the CoS value will be copied and used as the precedence value.

You can do the same for the QoS group-marking category. That is, you can configure the **set precedence qos-group** command, and the QoS group value will be copied and used as the precedence value.

The valid value range for the precedence value is a number from 0 to 7. The valid value range for the QoS group is a number from 0 to 99. Therefore, when configuring the **set precedence qos-group** command, note the following points:

- If a QoS group value falls within both value ranges (for example, 6), the packet-marking value will be copied and the packets will be marked.
- If QoS group value exceeds the precedence range (for example, 10), the packet-marking value will not be copied, and the packet will not be marked. No action is taken.

Precedence Values in IPv6 Environments

When this command is used in IPv6 environments it can set the value in both IPv4 and IPv6 packets. However, the actual packets set by this function are only those that meet the match criteria of the class-map containing this function.

Setting Precedence Values for IPv6 Packets Only

To set the precedence values for IPv6 packets only, the **match protocol ipv6** command must also be used in the class-map that classified packets for this action. Without the **match protocol ipv6** command, the class-map may classify both IPv6 and IPv4 packets, (depending on other match criteria) and the **set precedence** command will act upon both types of packets.

Setting Precedence Values for IPv4 Packets Only

To set the precedence values for IPv4 packets only, use a command involving the **ip** keyword like the **match ip precedence** or **match ip dscp** command or include the **match protocol ip** command along with the others in the class map. Without the additional **ip** keyword, the class-map may match both IPv6 and IPv4 packets (depending on the other match criteria) and the **set precedence** or **set dscp** command may act upon both types of packets.

Examples

In the following example, the policy map named policy-cos is created to use the values defined in a table map named table-map1. The table map named table-map1 was created earlier with the **table-map** (value mapping) command. For more information about the **table-map** (value mapping) command, see the **table-map** (value mapping) command page.

In this example, the precedence value will be set according to the CoS value defined in table-map1.

```
Router(config)# policy-map policy-cos
Router(config-pmap)# class class-default
Router(config-pmap-c)# set precedence cos table table-map1
Router(config-pmap-c)# end
```

The **set precedence** command is applied when you create a service policy in QoS policy-map configuration mode. This service policy is not yet attached to an interface or to an ATM virtual circuit. For information on attaching a service policy to an interface, refer to the "Modular Quality of Service Command-Line Interface Overview" chapter of the *Cisco IOS Quality of Service Solutions Configuration Guide.*

Related Commands

Command	Description
match dscp	Identifies a specific IP DSCP value as a match criterion.
match precedence	Identifies IP precedence values as match criteria.
match protocol	Configures the match criteria for a class map on the basis of the specified protocol.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
service-policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.
set cos	Sets the Layer 2 CoS value of an outgoing packet.
set dscp	Marks a packet by setting the Layer 3 DSCP value in the ToS byte.
set qos-group	Sets a group ID that can be used later to classify packets.
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 configuration for all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface.

Command	Description
show table-map	Displays the configuration of a specified table map or all table maps.
table-map (value mapping)	Creates and configures a mapping table for mapping and converting one packet-marking value to another.

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.

Command Default

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 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.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

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.

set vrf

To enable VPN routing and forwarding (VRF) instance selection within a route map for policy-based routing (PBR) VRF selection, use the **set vrf** command in route-map configuration mode. To disable VRF selection within a route map, use the **no** form of this command.

set vrf *vrf-name*

no set vrf *vrf-name*

Syntax Description

vrf-name	Name assigned to the VRF.

Command Default

VRF instance selection is not enabled within a route map for policy-based routing VRF selection.

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
12.2(33)SXI4	This command was modified. Support for IPv6 was added.

Usage Guidelines

The **set vrf** route-map configuration command was introduced with the Multi-VRF Selection Using Policy-Based Routing feature to provide a PBR mechanism for VRF selection. This command enables VRF selection by policy routing packets through a route map. The route map is attached to the incoming interface. The match criteria are defined in an IP access list or in an IP prefix list. The match criteria can also be defined based on the packet length with the **match length** route map command. The VRF must be defined before you configure this command, and the **ip policy route-map** interface configuration command must be configured to enable policy routing under the interface or subinterface. If the VRF is not defined or if policy routing is not enabled, an error message will be displayed on the console when you attempt to configure the **set vrf** command.

Note The **set vrf** command is not supported in hardware with the IP Services feature set. If this command is configured in IP Services, the packets are software switched. Hardware forwarding with this command in place requires packet circulation and is only supported in the Advanced IP Services feature set, which supports Multiprotocol Label Switching (MPLS).

In Cisco IOS Release 12.2(33)SXI4 on the Cisco Catalyst 6500, IPv6 PBR allows users to override normal destination IPv6 address-based routing and forwarding results. VRF allows multiple routing instances in Cisco IOS software. The PBR feature is VRF-aware, meaning that it works under multiple routing instances, beyond the default or global routing table.

In PBR, the **set vrf** command decouples the VRF and interface association and allows the selection of a VRF based on the ACL-based classification using the existing PBR or route-map configurations. It provides a single router with multiple routing tables and the ability to select routes based on the ACL classification. The router classifies packets based on ACL, selects a routing table, looks up the destination address, and then routes the packet.

Note The functionality provided by the **set vrf** and **set ip global next-hop** commands can also be configured with the **set default interface**, **set interface**, **set ip default next-hop**, and **set ip next-hop** commands. However, the **set vrf** and **set ip global next-hop** commands take precedence over the **set default interface**, **set interface**, **set ip default next-hop**, and **set ip next-hop** commands. No error message is displayed indicating that VRF is already enabled if you attempt to configure the **set vrf** command with any of these four **set** commands.

Examples

The following example shows a route-map sequence that selects and sets a VRF based on the match criteria defined in three different access lists. (The access list configuration is not shown in this example.) If the route map falls through and a match does not occur, the packet will be dropped if the destination is local.

```
route-map PBR-VRF-Selection permit 10
match ip address 40
set vrf VRF1
!
route-map PBR-VRF-Selection permit 20
match ip address 50
set vrf VRF2
!
route-map PBR-VRF-Selection permit 30
match ip address 60
set vrf VRF3
```

Related Commands

Command	Description
access-list (IP standard)	Defines a standard IP access list.
debug ip policy	Displays the IP policy routing packet activity.
ip policy route-map	Identifies a route map to use for policy routing on an interface.
ip vrf	Configures a VRF routing table.
ip vrf receive	Inserts the IP address of an interface as a connected route entry in a VRF routing table.
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.
match length	Bases policy routing on the Level 3 length of a packet.
route-map	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.

Command	Description
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and that have no explicit route to the destination.
set interface	Indicates where to forward packets that pass a match clause of a route map for policy routing.
set ip default next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing and for which the Cisco IOS software has no explicit route to a destination.
set ip next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing.

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.
12.2(50)SY	This command was modified. Information about IPv4 and IPv6 hardware statistics is displayed.

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.
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 access-list template

To display information about access control lists (ACLs), use the **show access-list template** command in privileged EXEC mode.

show access-list template {**summary** | *aclname* | **exceed** *number* | **tree**}

Syntax Description

summary	Displays summary information about ACLs.
aclname	Displays information about the specified ACL.
exceed *number*	Limits the results to template ACLs that replace more than the specified *number* of individual ACLs.
tree	Provides an easily readable summary of the frequency of use of each of the ACL types that the template ACL function sees.

Command Modes

Privileged EXEC#

Command History

Cisco IOS Release	Description
12.2(27)SBKA	This command was introduced on the Cisco 10000 series router.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Examples

This section provides examples of the different forms of the **show access-list template** command.

show access-list template summary

The following example shows output from the **show access-list template summary** command:

```
Router# show access-list template summary

Maximum rules per template ACL = 100
Templates active = 1
Number of ACLs those templates represent = 50
Number of tree elements = 1
```

Output from this command includes:

- Maximum number of rules per template ACL
- Number of discovered active templates
- Number of ACLs replaced by those templates

show access-list template *aclname*

The following example shows output from the **show access-list template** *aclname* command:

```
Router# show access-list template 4Temp_1073741891108

    Showing data for 4Temp_1073741891108
    4Temp_1073741891108 peer_ip used is 172.17.2.62,
    is a parent, attached acl count = 98
```

```
    currentCRC = 59DAB725


Router# show access-list template 4Temp_1342177340101

    Showing data for 4Temp_1342177340101
    4Temp_1342177340101 idb's ip peer = 172.17.2.55,
    parent is 4Temp_1073741891108, user account attached to parent = 98
    currentCRC = 59DAB725
```

Output from this display includes:

- Peer IP of the interface associated with the named template ACL
- Name of the ACL serving as the primary user of the named template ACL
- Number of ACLs matching the template of the named template ACL
- Current cyclic redundancy check 32-bit (CRC32) value

show access-list template exceed *number*

The following example shows output from the **show access-list template exceed** *number* command:

```
Router# show access-list template exceed 49
ACL name                        OrigCRC    Count     CalcCRC
4Temp_#120795960097             104FB543   50      104FB543
```

Table 50 describes the significant fields shown in the display.

Table 50 show access-list template exceed Field Descriptions

Field	Description
ACL Name	Name of the template ACL. Only template ACLs that contain more than the specified number (**exceed** *number*) of child ACLs are listed.
OrigCRC	Original CRC32 value
Count	Count of ACLs that match the template ACL
CalcCRC	Calculated CRC32 value

show access-list template tree

The following example shows output from the **show access-list template tree** command:

```
Router# show access-list template tree

ACL name              OrigCRC    Count   CalcCRC
4Temp_1073741891108   59DAB725   98      59DAB725
```

Table 51 describes the significant fields shown in the display.

Table 51 show access-list template tree Field Descriptions

Field	Description
ACL name	Name of an ACL on the Red-Black tree
OrigCRC	Original CRC32 value
Count	Number of users of the ACL
CalcCRC	Calculated CRC32 value

show adjacency

To display information about the Cisco Express Forwarding adjacency table or the hardware Layer 3-switching adjacency table, use the **show adjacency** command in user EXEC or privileged EXEC mode.

show adjacency [*ip-address*] [*interface-type interface-number* | **null** *number* | **port-channel** *number* | **sysclock** *number* | **vlan** *number* | *ipv6-address* | **fcpa** *number* | **serial** *number*] [**connectionid** *number*] [**link** {**ipv4** | **ipv6** | **mpls**}] [**detail** | **encapsulation**]

show adjacency summary [i*nterface-type interface-number*]

Syntax Description

ip-address	(Optional) An IP address or IPv6 address. **Note** On the Cisco 10000 series routers IPv6 is supported on Cisco IOS Release 12.2(28)SB or later releases.
interface-type interface-number	(Optional) Interface type and number. Valid values for the *interface-type* argument are **atm**, **async**, **auto-template**, **ctunnel, dialer**, **esconphy**, **fastethernet**, **filter**, **filtergroup**, **gigabitethernet**, **group-async**, **longreachethernet**, **loopback**, **mfr**, **multilink**, **portgroup**, **pos**, **tunnel**, **vif**, **virutal-template**, **voabypassin**, **voabypassout**, **voafilterin**, **voafilterout**, **voain**, and **voaout**. **Note** Not all interface types and numbers are available on all platforms. Enter the **show adjacency** command to verify the interface types for your platform.
null *number*	(Optional) Specifies the null interface. The valid value is **0**.
port-channel *number*	(Optional) Specifies the channel interface; valid values are 1 to 282.
sysclock *number*	(Optional) Telecom-bus clock controller; valid values are 1 to 6.
vlan *number*	(Optional) Specifies the VLAN; valid values are 1 to 4094.
ipv6-address	(Optional) Specifies the associated IPv6 address.
fcpa *number*	(Optional) The fiber channel; valid values are 1 to 6.
serial *number*	(Optional) Specifies the serial interface number; valid values are 1 to 6.
connectionid *number*	(Optional) Specifies the client connection identification number.
link {**ipv4** | **ipv6** | **mpls**}	(Optional) Specifies the link type (IP, IPv6, or Multiprotocol Label Switching (MPLS) traffic of the adjacency).
detail	(Optional) Displays the protocol detail and timer information.
summary	(Optional) Displays a summary of Cisco Express Forwarding adjacency information.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
11.2GS	This command was introduced.
11.1CC	Multiple platform support was added.
12.0(7)XE	Support was added for the Cisco 7600 series routers.
12.1(5c)EX	This command was modified to include Layer 3 information.
12.1(11b)E	The **atm**, **ge-wan**, and **pos** keywords were added.
12.2(8)T	The **detail** keyword output was modified to show the epoch value for each entry of the adjacency table. The **summary** keyword output was modified to show the table epoch for the adjacency table.
12.2(14)SX	Support for this command was added for 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(25)S	This command was integrated into Cisco IOS Release 12.2(25)S . The **link ipv4**, **link ipv6**, and **link mpls** keywords and the *prefix* argument were added.
12.2(28)SB	Support for IPv6 was added for the Cisco 10000 series routers.
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 implemented on Cisco ASR 1000 Series Aggregation Services Routers.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The **show adjacency** command is used to verify that an adjacency exists for a connected device, that the adjacency is valid, and that the MAC header rewrite string is correct.

For line cards, you must specify the line card if_number (interface number). Use the **show cef interface** command to obtain line card if_numbers.

You can use any combination of the *ip-address, interface-type*, and other keywords and arguments (in any order) as a filter to display a specific subset of adjacencies.

On Cisco 7600 series routers, hardware Layer 3-switching adjacency statistics are updated every 60 seconds.

Note On the Cisco 10000 series routers, Pv6 is supported on Cisco IOS Release 12.2(28)SB or later releases.

The following information may be displayed by the **show adjacency** commands:

- Protocol
- Interface
- Type of routing protocol that is configured on the interface
- Type of routed protocol traffic using this adjacency
- Next hop address
- Method of adjacency that was learned
- Adjacency source (for example, Address Resolution Protocol (ARP) or ATM Map)

- Encapsulation prepended to packet switched through this adjacency
- Chain of output chain elements applied to packets after an adjacency
- Packet and byte counts
- High availability (HA) epoch and summary event epoch
- MAC address of the adjacent router
- Time left before the adjacency rolls out of the adjacency table. After the adjacency rolls out, a packet must use the same next hop to the destination.

Examples

The following examples show how to display adjacency information:

Cisco 7500 Series Router

```
Router# show adjacency

Protocol Interface                Address
IP       FastEthernet2/3          172.20.52.1(3045)
IP       FastEthernet2/3          172.20.52.22(11)
```

The following example shows how to display adjacency information for a specific interface:

```
Router# show adjacency fastethernet 0/0

Protocol Interface                Address
IP       FastEthernet0/0          10.4.9.2(5)
IP       FastEthernet0/0          10.4.9.3(5)
```

Cisco 10000 Series Router

```
Router# show adjacency

Protocol Interface                Address
IP       FastEthernet2/0/0        172.20.52.1(3045)
IP       FastEthernet2/0/0        172.20.52.22(11)
```

Cisco 7500 and 10000 Series Router

The following example shows how to display detailed adjacency information for adjacent IPv6 routers:

```
Router# show adjacency detail

Protocol Interface                Address
IP       Tunnel0                  point2point(6)
                                   0 packets, 0 bytes
                                   00000000
                                   CEF   expires: 00:02:57
                                         refresh: 00:00:57
                                   Epoch: 0
IPV6     Tunnel0                  point2point(6)
                                   0 packets, 0 bytes
                                   00000000
                                   IPv6 CEF   never
                                   Epoch: 0
IPV6     Ethernet2/0              FE80::A8BB:CCFF:FE01:9002(3)
                                   0 packets, 0 bytes
                                   AABBCC019002AABBCC012C0286DD
                                   IPv6 ND    never
                                   Epoch: 0
IPV6     Ethernet2/0              3FFE:2002::A8BB:CCFF:FE01:9002(5)
                                   0 packets, 0 bytes
```

```
                                    AABBCC019002AABBCC012C0286DD
                                    IPv6 ND    never
                                    Epoch: 0
```

Table 52 describes the significant fields shown in the displays.

Table 52 show adjacency Field Descriptions

Field	Description
Protocol	Type of Internet protocol.
Interface	Outgoing interface.
Address	Next hop IP address.

The following example shows how to display a summary of adjacency information:

```
Router# show adjacency summary

Adjacency table has 7 adjacencies:
  each adjacency consumes 368 bytes (4 bytes platform extension)
  6 complete adjacencies
  1 incomplete adjacency
  4 adjacencies of linktype IP
    4 complete adjacencies of linktype IP
    0 incomplete adjacencies of linktype IP
    0 adjacencies with fixups of linktype IP
    2 adjacencies with IP redirect of linktype IP
  3 adjacencies of linktype IPV6
    2 complete adjacencies of linktype IPV6
    1 incomplete adjacency of linktype IPV6

Adjacency database high availability:
  Database epoch: 8 (7 entries at this epoch)

Adjacency manager summary event processing:
 Summary events epoch is 52
 Summary events queue contains 0 events (high water mark 113 events)
 Summary events queue can contain 49151 events
 Adj last sourced field refreshed every 16384 summary events
RP adjacency component enabled
```

The following examples show how to display protocol detail and timer information:

For a Cisco 7500 Series Router

```
Router# show adjacency detail

Protocol Interface                Address
IP       FastEthernet0/0          10.4.9.2(5)
                                  0 packets, 0 bytes
                                  epoch 0
                                  sourced in sev-epoch 2
                                  Encap length 14
                                  00307131ABFC000500509C080800
                                  ARP
IP       FastEthernet0/0          10.4.9.3(5)
                                  0 packets, 0 bytes
                                  epoch 0
                                  sourced in sev-epoch 2
                                  Encap length 14
                                  000500506C08000500509C080800
```

```
                                  ARP
```

For a Cisco 7600 Series Router

```
Router# show adjacency detail

Protocol Interface                Address
IP       FastEthernet2/3          172.20.52.1(3045)
                                  0 packets, 0 bytes
                                  000000000FF920000380000000000000
                                  000000000000000000000000000000000
                                  00605C865B2800D0BB0F980B0800
                                  ARP        03:58:12
IP       FastEthernet2/3          172.20.52.22(11)
                                  0 packets, 0 bytes
                                  000000000FF920000380000000000000
                                  000000000000000000000000000000000
                                  00801C93804000D0BB0F980B0800
                                  ARP        03:58:06
```

For a Cisco 10000 Series Router

```
Router# show adjacency detail

Protocol Interface                Address
IP       FastEthernet2/0/0          10.4.9.2(5)
                                  0 packets, 0 bytes
                                  epoch 0
                                  sourced in sev-epoch 2
                                  Encap length 14
                                  00307131ABFC000500509C080800
                                  ARP
IP       FastEthernet2/0/0          10.4.9.3(5)
                                  0 packets, 0 bytes
                                  epoch 0
                                  sourced in sev-epoch 2
                                  Encap length 14
                                  000500506C08000500509C080800
                                  ARP
```

The following examples show how to display protocol detail and timer adjacency information for IP links for a specific interface:

For a Cisco 7500 Series Router

```
Router# show adjacency tunnel 1 link detail

Protocol Interface                Address
IP       Tunnel1                  point2point(7)
                                  0 packets, 0 bytes
                                  epoch 1
                                  sourced in sev-epoch 4
                                  empty encap string
                                  P2P-ADJ
                                  Next chain element:
                                   label 16 TAG adj out of Ethernet1/0, addr 10.0.0.0
```

For a Cisco 7600 Series Router

```
Router# show adjacency fastethernet 2/3

Protocol Interface                Address
IP       FastEthernet2/3          172.20.52.1(3045)
IP       FastEthernet2/3          172.20.52.22(11)
```

For a Cisco 10000 Series Router

```
Router# show adjacency tunnel 1 link detail

Protocol Interface              Address
IP       Tunnel1                point2point(7)
                                0 packets, 0 bytes
                                epoch 1
                                sourced in sev-epoch 4
                                empty encap string
                                P2P-ADJ
                                Next chain element:
                                label 16 TAG adj out of FastEthernet0/0, addr 10.0.0.0
```

Related Commands

Command	Description
clear adjacency	Clears the Cisco Express Forwarding adjacency table.
clear arp-cache	Deletes all dynamic entries from the ARP cache.
show adjacency	Enables the display of information about the adjacency database.
show mls cef adjacency	Displays information about the hardware Layer 3-switching adjacency node.
show cef interface	Displays detailed Cisco Express Forwarding information for all interfaces.

show atm map

To display the list of all configured ATM static maps to remote hosts on an ATM network and on ATM bundle maps, use the **show atm map** command in user EXEC or privileged EXEC mode.

show atm map

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
11.1CA	This command was modified to include an example for the ATM-CES port adapter (PA).
12.0(3)T	This command was modified to include display for ATM bundle maps. An ATM bundle map identifies a bundle and all of its related virtual circuits (VCs).
12.2(2)T	The display output for this command was modified to include the IPv6 address mappings of remote nodes to ATM permanent virtual circuits (PVCs).
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 Release 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.

Examples

The following is sample output from the **show atm map** command for a bundle called san-jose (0/122, 0/123, 0/124, and 0/126 are the virtual path and virtual channel identifiers of the bundle members):

```
Router# show atm map

Map list san-jose_B_ATM1/0.52 : PERMANENT
ip 10.1.1.1. maps to bundle san-jose, 0/122, 0/123, 0/124, 0/126, ATM1/0.52, broadcast
```

The following is sample output from the **show atm map** command for an ATM-CES PA on the Cisco 7200 series router:

```
Router# show atm map

Map list alien: PERMANENT
ip 10.1.1.1 maps to VC 6
ip 10.1.1.2 maps to VC 6
```

The following is sample output from the **show atm map** command that displays information for a bundle called new-york:

```
Router# show atm map

Map list atm:
vines 3004B310:0001 maps to VC 4, broadcast
ip 172.21.168.110 maps to VC 1, broadcast
clns 47.0004.0001.0000.0c00.6e26.00 maps to VC 6, broadcast
appletalk 10.1 maps to VC 7, broadcast
decnet 10.1 maps to VC 2, broadcast
Map list new-york: PERMANENT
ip 10.0.0.2 maps to bundle new-york, 0/200, 0/205, 0/210, ATM1/0.1
```

The following is sample output from the **show atm map** command for a multipoint connection:

```
Router# show atm map

Map list atm_pri: PERMANENT
ip 10.4.4.4 maps to NSAP CD.CDEF.01.234567.890A.BCDE.F012.3456.7890.1234.12, broadcast,
aal5mux, multipoint connection up, VC 6
ip 10.4.4.6 maps to NSAP DE.CDEF.01.234567.890A.BCDE.F012.3456.7890.1234.12, broadcast,
aal5mux, connection up, VC 15, multipoint connection up, VC 6

Map list atm_ipx: PERMANENT
ipx 1004.dddd.dddd.dddd maps to NSAP DE.CDEF.01.234567.890A.BCDE.F012.3456.7890.1234.12,
broadcast, aal5mux, multipoint connection up, VC 8
ipx 1004.cccc.cccc.cccc maps to NSAP CD.CDEF.01.234567.890A.BCDE.F012.3456.7890.1234.12,
broadcast, aal5mux, multipoint connection up, VC 8

Map list atm_apple: PERMANENT
appletalk 62000.5 maps to NSAP CD.CDEF.01.234567.890A.BCDE.F012.3456.7890.1234.12,
broadcast, aal5mux, multipoint connection up, VC 4
appletalk 62000.6 maps to NSAP DE.CDEF.01.234567.890A.BCDE.F012.3456.7890.1234.12,
broadcast, aal5mux, multipoint connection up, VC 4
```

The following is sample output from the **show atm map** command if you configure an ATM PVC using the **pvc** command:

```
Router# show atm map

Map list endA: PERMANENT
ip 10.11.11.1 maps to VC 4, VPI 0, VCI 60, ATM0.2
```

The following sample output from the **show atm map** command shows the link-local and global IPv6 addresses (FE80::60:3E47:AC8:C and 2001:0DB8:2222::72, respectively) of a remote node that are explicitly mapped to PVC 1/32 of ATM interface 0;

```
Router# show atm map

Map list ATM0pvc1 : PERMANENT
ipv6 FE80::60:3E47:AC8:C maps to VC 1, VPI 1, VCI 32, ATM0
        , broadcast
ipv6 2001:0DB8:2222::72 maps to VC 1, VPI 1, VCI 32, ATM0
```

Table 53 describes the significant fields shown in the displays.

Table 53 show atm map Field Descriptions

Field	Description
Map list	Name of map list.
PERMANENT	This map entry was entered from configuration; it was not entered automatically by a process.
ip 172.21.168.110 maps to VC 1 or ip 10.4.4.6 maps to NSAP DE.CDEF.01.234567.890A.BCDE.F012.3456.7890.1234.12	Name of protocol, the protocol address, and the virtual circuit descriptor (VCD) or network service access point (NSAP) to which the address is mapped (for ATM VCs configured with the **atm pvc** command).
broadcast	Indicates pseudobroadcasting.
ip 10.11.11.1 maps to VC 4, VPI 0, VCI 60, ATM0.2 or	Name of protocol, the protocol address, the virtual path identifier (VPI) number, the virtual channel identifier (VCI) number, and the ATM interface or subinterface (for ATM PVCs configured using the **pvc** command). or
ip 10.4.4.6 maps to NSAP DE.CDEF.01.234567.890A.BCDE.F012.3456.7890.1234.12	Name of the protocol, the protocol address, and the NSAP to which the address is mapped (for ATM switched virtual circuits (SVCs) configured using the **svc** command).
aal5mux	Indicates the encapsulation used, a multipoint or point-to-point VC, and the number of the virtual circuit.
multipoint connection up	Indicates that this is a multipoint VC.
VC 6	Number of the VC.
connection up	Indicates a point-to-point VC.
VPI	VPI for the VC.
VCI	VCI for the VC.
ATM1/0.52	ATM interface or subinterface number.
Map list	Name of the bundle whose mapping information follows.
ip 10.1.1.1 maps to bundle san-jose, 0/122, 0/123, 0/124, 0/126	IP address of the bundle and VC members that belong to the bundle.

Related Commands

Command	Description
protocol (ATM)	Configures a static map for an ATM PVC, SVC, VC class, or VC bundle. Enables Inverse ARP or Inverse ARP broadcasts on an ATM PVC by either configuring Inverse ARP directly on the PVC, on the VC bundle, or in a VC class (applies to IP and IPX protocols only).
protocol ipv6 (ATM)	Maps the IPv6 address of a remote node to the ATM PVC used to reach the address.

Command	Description
pvc	Creates or assigns a name to an ATM PVC, specifies the encapsulation type on an ATM PVC, or enters interface-ATM-VC configuration mode.
show atm bundle	Displays the bundle attributes assigned to each bundle VC member and the current working status of the VC members.
show atm bundle statistics	Displays statistics on the specified bundle.
svc	Creates an ATM SVC and specifies destination NSAP address on an interface or subinterface.

show bfd neighbors

To display a line-by-line listing of existing Bidirectional Forwarding Detection (BFD) adjacencies, use the **show bfd neighbors** command in user EXEC or privileged EXEC mode.

show bfd neighbors [**client** {**bgp** | **eigrp** | **isis** | **ospf** | **rsvp** | **te-frr**} | **details** | [*interface-type interface-number*] | **internal** | **ipv4** *ip-address* | **ipv6** *ipv6-address* | **vrf** *vrf-name*]

Syntax Description

client	(Optional) Displays the neighbors of a specific client.
bgp	(Optional) Specifies a Border Gateway Protocol (BGP) client.
eigrp	(Optional) Specifies an Enhanced Interior Gateway Routing Protocol (EIGRP) client.
isis	(Optional) Specifies an Intermediate System-to-Intermediate System (IS-IS) client.
ospf	(Optional) Specifies an Open Shortest Path First (OSPF) client.
rsvp	(Optional) Specifies a Resource Reservation Protocol (RSVP) client.
te-frr	(Optional) Specifies a Traffic Engineering (TE) Fast Reroute (FRR) client.
details	(Optional) Displays all BFD protocol parameters and timers for each neighbor.
interface-type interface-number	(Optional) Neighbors at a specified interface.
internal	(Optional) Displays internal BFD information.
ipv4	(Optional) Specifies an IPv4 neighbor. If the **ipv4** keyword is used without the *ip-address* argument, all IPv4 sessions are displayed.
ip-address	(Optional) IP address of a neighbor in A.B.C.D format.
ipv6	(Optional) Specifies an IPv6 neighbor. If the **ipv6** keyword is used without the *ipv6-address* argument, all IPv6 sessions are displayed.
ipv6-address	(Optional) IPv6 address of a neighbor in X:X:X:X::X format.
vrf *vrf-name*	(Optional) Displays entries for a specific Virtual Private Network (VPN) routing and forwarding (VRF) instance.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

S Release	Modification
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S.
12.2(18)SXE	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRC	This command was modified. The **vrf** *vrf-name* keyword and argument, the **client** keyword, and the *ip-address* argument were added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was modified. The output was modified to display the "OurAddr" field only with the **details** keyword.

12.2(33)SRE	This command was modified. Support for IPv6 was added.
15.1(2)S	This command was modified. • The **show bfd neighbors details** command output was changed for hardware-offloaded BFD sessions. • The **show bfd neighbors** command output was changed to show the header type identifying the session type.
T Release	**Modification**
12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.
12.4(9)T	This command was modified. Support for BFD Version 1 and BFD echo mode was added.
15.1(2)T	This command was modified. Support for IPv6 was added.
X Release	**Modification**
Cisco IOS XE Release 2.1	This command was modified. Support for IPv6 was added.

Usage Guidelines

The **show bfd neighbors** command can be used to help troubleshoot the BFD feature.

The full output for the **details** keyword is not supported on the Route Processor (RP) for the Cisco 12000 series Internet router. If you want to enter the **show bfd neighbors** command with the **details** keyword on the Cisco 12000 series Internet router, you must enter the command on the line card. Use the **attach** *slot* command to establish a CLI session with a line card.

In Cisco IOS Release 15.1(2)S and later releases that support BFD hardware offload, the Tx and Rx intervals on both BFD peers must be configured in multiples of 50 milliseconds. If they are not, output from the **show bfd neighbors details** command will show the configured intervals, not the changed ones.

See the "Configuring Synchronous Ethernet on the Cisco 7600 Router with ES+ Line Card" section of the *Cisco 7600 Series Ethernet Services Plus (ES+) and Ethernet Services Plus T (ES+T) Line Card Configuration Guide* for more information about prerequisites and restrictions for hardware offload.

Examples

Examples for Cisco IOS Release 12.0(31)S, 12.2(18)SXE, 12.2(33)SRA, 12.2(33)SB, and 12.4(4)T

The following sample output shows the status of the adjacency or neighbor:

```
Router# show bfd neighbors

OurAddr       NeighAddr      LD/RD RH  Holdown(mult) State     Int
172.16.10.1   172.16.10.2    1/6  1    260   (3 )      Up        Fa0/1
```

The following sample output from the **show bfd neighbors** command entered with the **details** keyword shows BFD protocol parameters and timers for each neighbor:

```
Router# show bfd neighbors details

NeighAddr                          LD/RD    RH/RS     State     Int
10.1.1.2                            1/1         1(RH) Up        Et0/0
Session state is UP and not using echo function.
OurAddr: 10.1.1.1
Local Diag: 0, Demand mode: 0, Poll bit: 0
```

```
MinTxInt: 50000, MinRxInt: 50000, Multiplier: 3 Received MinRxInt: 50000, Received
Multiplier: 3 Holddown (hits): 150(0), Hello (hits): 50(2223) Rx Count: 2212, Rx Interval
(ms) min/max/avg: 8/68/49 last: 0 ms ago Tx Count: 2222, Tx Interval (ms) min/max/avg:
40/60/49 last: 20 ms ago Elapsed time watermarks: 0 0 (last: 0) Registered protocols: CEF
Stub
Uptime: 00:01:49
Last packet: Version: 0                  - Diagnostic: 0
             I Hear You bit: 1           - Demand bit: 0
             Poll bit: 0                 - Final bit: 0
             Multiplier: 3               - Length: 24
             My Discr.: 1                - Your Discr.: 1
             Min tx interval: 50000      - Min rx interval: 50000
             Min Echo interval: 50000
```

The following sample output from the RP on a Cisco 12000 series Internet router shows the status of the adjacency or neighbor:

```
Router# show bfd neighbors

Cleanup timer hits: 0

OurAddr       NeighAddr     LD/RD RH  Holdown(mult)  State     Int
172.16.10.2   172.16.10.1    2/0  0   0    (0 )      Up        Fa6/0
 Total Adjs Found: 1
```

The following sample output from the RP on a Cisco 12000 series Internet router shows the status of the adjacency or neighbor with the **details** keyword:

```
Router# show bfd neighbors details

Cleanup timer hits: 0

OurAddr       NeighAddr     LD/RD RH  Holdown(mult)  State     Int
172.16.10.2   172.16.10.1    2/0  0   0    (0 )      Up        Fa6/0
Registered protocols: OSPF
Uptime: never
%% BFD Neighbor statistics are not available on RP. Please execute this command on Line
Card.
```

The following sample output from a line card on a Cisco 12000 series Internet router shows the status of the adjacency or neighbor:

```
Router# attach 6

Entering Console for 8 Port Fast Ethernet in Slot: 6
Type "exit" to end this session

Press RETURN to get started!

Router> show bfd neighbors

Cleanup timer hits: 0

OurAddr       NeighAddr     LD/RD RH  Holdown(mult)  State     Int
172.16.10.2   172.16.10.1    2/1  1   848  (5 )      Up        Fa6/0
 Total Adjs Found: 1
```

The following sample output from a line card on a Cisco 12000 series Internet router shows the status of the adjacency or neighbor with the **details** keyword:

```
Router# attach 6

Entering Console for 8 Port Fast Ethernet in Slot: 6
Type "exit" to end this session
```

```
Press RETURN to get started!

Router> show bfd neighbors details

Cleanup timer hits: 0

OurAddr       NeighAddr     LD/RD RH  Holdown(mult)  State     Int
172.16.10.2   172.16.10.1    2/1  1   892  (5 )      Up        Fa6/0
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 1000, Multiplier: 3
Received MinRxInt: 200000, Received Multiplier: 5
Holdown (hits): 1000(0), Hello (hits): 200(193745)
Rx Count: 327406, Rx Interval (ms) min/max/avg: 152/248/196 last: 108 ms ago
Tx Count: 193748, Tx Interval (ms) min/max/avg: 204/440/331 last: 408 ms ago
Last packet: Version: 0            - Diagnostic: 0
             I Hear You bit: 1     - Demand bit: 0
             Poll bit: 0           - Final bit: 0
             Multiplier: 5         - Length: 24
             My Discr.: 1          - Your Discr.: 2
             Min tx interval: 200000    - Min rx interval: 200000
             Min Echo interval: 0
Uptime: 17:54:07
SSO Cleanup Timer called: 0
SSO Cleanup Action Taken: 0
Pseudo pre-emptive process count: 7728507 min/max/avg: 8/16/8 last: 12 ms ago
 IPC Tx Failure Count: 0
 IPC Rx Failure Count: 0
 Total Adjs Found: 1
LC-Slot6>
```

Example for 12.4(9)T and Later Releases

The following sample output verifies that the BFD neighbor router is also running BFD Version 1 and that the BFD session is up and running in echo mode:

```
Router# show bfd neighbors details

OurAddr       NeighAddr     LD/RD  RH/RS   Holdown(mult)  State     Int
172.16.1.2    172.16.1.1     1/6    Up        0    (3 )   Up        Fa0/1
Session state is UP and using echo function with 50 ms interval.
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3
Received MinRxInt: 1000000, Received Multiplier: 3
Holdown (hits): 3000(0), Hello (hits): 1000(337)
Rx Count: 341, Rx Interval (ms) min/max/avg: 1/1008/882 last: 364 ms ago
Tx Count: 339, Tx Interval (ms) min/max/avg: 1/1016/886 last: 632 ms ago
Registered protocols: EIGRP
Uptime: 00:05:00
Last packet: Version: 1            - Diagnostic: 0
             State bit: Up         - Demand bit: 0
             Poll bit: 0           - Final bit: 0
             Multiplier: 3         - Length: 24
             My Discr.: 6          - Your Discr.: 1
             Min tx interval: 1000000    - Min rx interval: 1000000
             Min Echo interval: 50000
```

Example for Cisco IOS XE Release 2.1 and Later Releases

The following example displays all IPv6 sessions:

```
Router# show bfd neighbors ipv6 2001::1

OurAddr    NeighAddr  LD/RD  RH/RS  Holddown(mult)  State  Int
1:1::5     1:1::6      2/2    Up        0    (3 )   Up     Et0/0
```

```
2:2::5     2:2::6      4/4     Up         0     (3 )   Up      Et1/0
```

Examples for Cisco IOS Release 12.2(33)SXI, 12.2(33)SRE, 12.2(33)XNA, and Later Releases

The following is sample output from the **show bfd neighbors** command:

```
Router# show bfd neighbors

NeighAddr                              LD/RD    RH/RS     State     Int
192.0.2.1                               4/0     Down      Down      Et0/0
192.0.2.2                               5/0     Down      Down      Et0/0
192.0.2.3                               6/0     Down      Down      Et0/0
192.0.2.4                               7/0     Down      Down      Et0/0
192.0.2.5                               8/0     Down      Down      Et0/0
192.0.2.6                              11/0         0(RH) Fail      Et0/0
1000:1:1:1:1:1:1:2                      9/0     Down      Down      Et0/0
1000:1:1:1:1:1:1:810                   10/0     Down      Down      Et0/0
1000:1111:1111:111:11:111:11:5          1/0         0(RH) Fail      Et0/0
1000:1111:1111:111:11:111:11:6          2/0     Down      Down      Et0/0
1000:1111:1111:1111:1111:1111:1111:8810
                                        3/0     Down      Down      Et0/0
```

The following is sample output from the **show bfd neighbors details** command:

```
Router# show bfd neighbors details

NeighAddr                              LD/RD    RH/RS     State     Int
192.0.2.5                               4/0     Down      Down      Et0/0
OurAddr: 192.0.2.8
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3
Received MinRxInt: 0, Received Multiplier: 0
Holddown (hits): 0(0), Hello (hits): 1000(120)
Rx Count: 0, Rx Interval (ms) min/max/avg: 0/0/0 last: 118672 ms ago
Tx Count: 120, Tx Interval (ms) min/max/avg: 760/1000/885 last: 904 ms ago
Elapsed time watermarks: 0 0 (last: 0)
Registered protocols: Stub
Last packet: Version: 1             - Diagnostic: 0
             State bit: AdminDown   - Demand bit: 0
             Poll bit: 0            - Final bit: 0
             Multiplier: 0          - Length: 0
             My Discr.: 0           - Your Discr.: 0
             Min tx interval: 0     - Min rx interval: 0
             Min Echo interval: 0


NeighAddr                              LD/RD    RH/RS     State     Int
1000:1:1:1:1:1:1:2                      9/0     Down      Down      Et0/0
OurAddr: 1000:1:1:1:1:1:1:1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3
Received MinRxInt: 0, Received Multiplier: 0
Holddown (hits): 0(0), Hello (hits): 1000(208)
Rx Count: 0, Rx Interval (ms) min/max/avg: 0/0/0 last: 194760 ms ago
Tx Count: 208, Tx Interval (ms) min/max/avg: 760/1000/878 last: 424 ms ago
Elapsed time watermarks: 0 0 (last: 0)
Registered protocols: Stub
Last packet: Version: 1             - Diagnostic: 0
             State bit: AdminDown   - Demand bit: 0
             Poll bit: 0            - Final bit: 0
             Multiplier: 0          - Length: 0
             My Discr.: 0           - Your Discr.: 0
             Min tx interval: 0     - Min rx interval: 0
```

```
Min Echo interval: 0
```

Table 54 describes the significant fields shown in the displays.

Table 54 show bfd neighbors Field Descriptions

Field	Description
OurAddr	IP address of the interface for which the **show bfd neighbors details** command was entered.
NeighAddr	IPv4 or IPv6 address of the BFD adjacency or neighbor.
LD/RD	Local discriminator and remote discriminator being used for the session.
RH	Remote Heard—Indicates that the remote BFD neighbor has been heard.
Holdown(mult)	The detect timer multiplier that is used for this session.
State	State of the interface—Up or Down.
Int	Interface type and slot/port.
Session state is UP and using echo function with 50 ms interval.	BFD is up and running in echo mode. The 50-millisecond interval has been adopted from the **bfd** command. **Note** BFD Version 1 and echo mode are supported only with Cisco IOS Release 12.4(9)T and later releases.
Rx Count	Number of BFD control packets that have been received from the BFD neighbor.
Tx Count	Number of BFD control packets that have been sent by the BFD neighbor.
Tx Interval	The interval, in milliseconds, between sent BFD packets.
Registered protocols	Routing protocols that have been registered with BFD.
Last packet: Version:	BFD version detected and run between the BFD neighbors. The system automatically performs BFD version detection, and BFD sessions between neighbors will run in the highest common BFD version between neighbors. For example, if one BFD neighbor is running BFD Version 0, and the other BFD neighbor is running Version 1, the session will run BFD Version 0. **Note** BFD Version 1 and echo mode are supported only with Cisco IOS Release 12.4(9)T and later releases.
Diagnostic	A diagnostic code specifying the local system's reason for the last transition of the session from Up to some other state. State values are as follows: • 0—No Diagnostic • 1—Control Detection Time Expired • 2—Echo Function Failed • 3—Neighbor Signaled Session Down • 4—Forwarding Plane Reset • 5—Path Down • 6—Concentrated Path Down • 7—Administratively Down

Table 54 show bfd neighbors Field Descriptions (continued)

Field	Description
I Hear You bit	The I Hear You Bit is set to 0 if the transmitting system is either not receiving BFD packets from the remote system or is tearing down the BFD session for some reason. During normal operation, the I Hear You bit is set to 1 to signify that the remote system is receiving the BFD packets from the transmitting system.
Demand bit	Demand Mode bit. BFD has two modes—asynchronous and demand. If the Demand Mode is set, the transmitting system prefers to operate in demand mode. The Cisco implementation of BFD supports only asynchronous mode.
Poll bit	If the Poll bit is set, the transmitting system is requesting verification of connectivity or verification of a parameter change.
Final bit	If the Final bit is set, the transmitting system is responding to a received BFD control packet that had a Poll (P) bit set.
Multiplier	Detect time multiplier. The negotiated transmit interval multiplied by the detect time multiplier determines the detection time for the transmitting system in BFD asynchronous mode. The detect time multiplier is similar to the hello multiplier in Intermediate System-to-Intermediate System (IS-IS), which is used to determine the hold timer: (hello interval) * (hello multiplier) = hold timer. If a hello packet is not received within the hold-timer interval, a failure has occurred. Similarly, for BFD: (transmit interval) * (detect multiplier) = detect timer. If a BFD control packet is not received from the remote system within the detect-timer interval, a failure has occurred.
Length	Length of the BFD control packet, in bytes.
My Discr.	My Discriminator. Unique, nonzero discriminator value generated by the transmitting system used to demultiplex multiple BFD sessions between the same pair of systems.
Your Discr.	Your Discriminator. The discriminator received from the corresponding remote system. This field reflects the received value of My Discriminator, or is zero if that value is unknown.
Min tx interval	Minimum transmission interval, in microseconds, that the local system wants to use when sending BFD control packets.
Min rx interval	Minimum receipt interval, in microseconds, between received BFD control packets that the system can support.
Min Echo interval	Minimum interval, in microseconds, between received BFD control packets that the system can support. If the value is zero, the transmitting system does not support the receipt of BFD echo packets. The Cisco implementation of BFD for Cisco IOS Releases 12.2(18)SXE and 12.0(31)S does not support the use of echo packets.

Example for Cisco IOS Release 15.1(2)S with Hardware Offload to Cisco 7600 Series Routers

The following is sample output from the **show bfd neighbors details** command for BFD sessions offloaded to hardware. The Rx and Tx counts show the number of packets received and transmitted by the BFD session in hardware.

```
NeighAddr                              LD/RD         RH/RS     State     Int
192.0.2.1                              298/298        Up        Up        Te7/1.2
Session state is UP and not using echo function.
Session Host: Hardware - session negotiated with platform adjusted timer values.
              Holddown - negotiated: 510000      adjusted: 0
OurAddr: 192.0.2.2
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 170000, MinRxInt: 170000, Multiplier: 3
Received MinRxInt: 160000, Received Multiplier: 3
Holddown (hits): 0(0), Hello (hits): 170(0)
Rx Count: 1256983
Tx Count: 24990
Elapsed time watermarks: 0 0 (last: 0)
Registered protocols: OSPF CEF
Uptime: 18:11:31
Last packet: Version: 1                  - Diagnostic: 0
             State bit: Up               - Demand bit: 0
             Poll bit: 0                 - Final bit: 0
             Multiplier: 3               - Length: 24
             My Discr.: 298                - Your Discr.: 298
             Min tx interval: 160000     - Min rx interval: 160000
             Min Echo interval: 0
```

Examples for Cisco IOS Release 15.1(2)S with Changes in the Header Line in the Output

The following is sample output from the **show bfd neighbors** command showing a header type identifying the type of session:

```
Router# show bfd neighbors

MPLS-TP Sessions
Interface       LSP type                 LD/RD    RH/RS     State
Tunnel-tp1      Working                   1/0     Down      Down
Tunnel-tp2      Working                   3/0     Down      Down
Tunnel-tp1      Protect                   2/0     Down      Down


IPv4 Sessions
NeighAddr                          LD/RD    RH/RS     State     Int
192.0.2.1                            2/0     Down      Down      Et2/0
```

The following is sample output from the **show bfd neighbors** command for Virtual Circuit Connection Verification (VCCV) sessions:

```
Router# show bfd neighbors

VCCV Sessions
Peer Addr      :VCID                    LD/RD    RH/RS     State
198.51.100.1   :100                      1/1     Up        Up
```

The following is sample output from the **show bfd neighbors** command for IPv4 and IPv6 sessions:

```
Router# show bfd neighbors

IPv4 Sessions
NeighAddr                            LD/RD    RH/RS     State     Int
192.0.2.1                             6/0     Down      Down      Et1/0
203.0.113.1                           7/6     Up        Up        Et3/0
198.51.100.2                          8/7     Up        Up        Et0/0

IPv6 Sessions
NeighAddr                          LD/RD    RH/RS     State     Int
CC::2                               1/1     Up        Up        Et0/0
```

```
DD::2                                     2/2      Up         Up         Et0/0
EE::2                                     3/3      Up         Up         Et0/0
ABCD::2                                   4/4      Up         Up         Et0/0
FE80::2                                   5/5      Up         Up         Et0/0
```

Table 55 describes the significant fields shown in the displays.

Table 55 show bfd neighbors Field Descriptions

Field	Description
Interface	Name of the MPLS tunnel TP interface.
LSP type	Type of label switched path for this session (Working or Protect).

Related Commands

Command	Description
attach	Connects to a specific line card to execute monitoring and maintenance commands on that line card.

show bfd summary

To display summary information for Bidirectional Forwarding Protocol (BFD), use the **show bfd summary** command in user EXEC or privileged EXEC mode.

show bfd summary [**client** | **session**]

Syntax Description

client	(Optional) Displays list of BFD clients and number of sessions created by each client.
session	(Optional) Displays list of client-to-peer exchanges that have been launched by BFD clients, organized by session type.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

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

Usage Guidelines

Use this command to display summary information about BFD, BFD clients, or BFD sessions.

When a BFD client launches a session with a peer, BFD sends periodic BFD control packets to the peer. Information about the following states of a session are included in the output of this command:

- Up—When another BFD interface acknowledges the BFD control packets, the session moves into an up state.
- Down—The session, and data path, is declared down if a data path failure occurs and BFD does not receive a control packet within the configured amount of time. When a session is down, BFD notifies the BFD client so that the client can perform necessary actions to reroute traffic.

Examples

The following is sample output from the **show bfd summary** command:

```
Router# show bfd summary

                    Session          Up          Down

Total                     1           1             0
```

The following is sample output from the **show bfd summary session** command:

```
Router# show bfd summary session

Protocol            Session          Up          Down
IPV4                      1           1             0

Total                     1           1             0
```

The following is sample output from the **show bfd summary client** command:

```
Router# show bfd summary client
```

```
Client               Session          Up          Down
EIGRP                      1           1             0
CEF                        1           1             0

Total                      2           2             0
```

Table 56 describes the significant fields shown in the display.

Table 56 show bfd summary Field Descriptions

Field	Description
Session	Sum of launched sessions by type or when combined with Total, sum of all launched sessions.
Up	Number of sessions for which the BFD client acknowleged receipt of control packets.
Down	Number of sessions for which the BFD client did not receive control packets from a peer.
Total	Sum of all launched sessions, all Up sessions, or all Down sessions in list.
Protocol	Routing protocol of interface in a session.
Client	Type of client in a session.

Related Commands

Command	Description
show bfd neighbors	Displays list of existing BFD adjacencies.

show bgp ipv6

To display entries in the IPv6 Border Gateway Protocol (BGP) routing table, use the **show bgp ipv6** command in user EXEC or privileged EXEC mode.

show bgp ipv6 {**unicast** | **multicast**} [*ipv6-prefix*/*prefix-length*] [**longer-prefixes**] [**labels**]

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.
ipv6-prefix	(Optional) IPv6 network number, entered to display a particular network in the IPv6 BGP routing table. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/prefix-length	(Optional) The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
longer-prefixes	(Optional) Displays the route and more specific routes.
labels	(Optional) Displays Multiprotocol Label Switching (MPLS) label information.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(2)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	MPLS label information was added to the display.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(2)T	MPLS label value advertised for the IPv6 prefix was added to the display.
12.0(26)S	The **unicast** and **multicast** keywords were added.
12.2(25)S	6PE multipath information was added to the display.
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.
12.2(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 introduced on Cisco ASR 1000 series routers.

Usage Guidelines

The **show bgp ipv6** command provides output similar to the **show ip bgp** command, except that it is IPv6-specific.

Examples

The following is sample output from the **show bgp ipv6** command:

```
Router# show bgp ipv6 unicast

BGP table version is 12612, local router ID is 172.16.7.225
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*                   3FFE:C00:E:C::2                        0 3748 4697 1752 i
*                   3FFE:1100:0:CC00::1
                                                           0 1849 1273 1752 i
*  2001:618:3::/48  3FFE:C00:E:4::2          1             0 4554 1849 65002 i
*>                  3FFE:1100:0:CC00::1
                                                           0 1849 65002 i
*  2001:620::/35    2001:0DB8:0:F004::1
                                                           0 3320 1275 559 i
*                   3FFE:C00:E:9::2                        0 1251 1930 559 i
*                   3FFE:3600::A                           0 3462 10566 1930 559 i
*                   3FFE:700:20:1::11
                                                           0 293 1275 559 i
*                   3FFE:C00:E:4::2          1             0 4554 1849 1273 559 i
*                   3FFE:C00:E:B::2                        0 237 3748 1275 559 i
```

Table 57 describes the significant fields shown in the display.

Table 57 show bgp ipv6 Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	A 32-bit number written as 4 octets separated by periods (dotted decimal format).
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s—The table entry is suppressed. • d—The table entry is dampened. • h—The table entry is history. • *—The table entry is valid. • >—The table entry is the best entry to use for that network. • i—The table entry was learned via an internal BGP session.
Origin codes	Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: • i—Entry originated from the Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • e—Entry originated from the Exterior Gateway Protocol (EGP). • ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IPv6 address of a network entity.

Table 57 show bgp ipv6 Field Descriptions (continued)

Field	Description
Next Hop	IPv6 address of the next system that is used when forwarding a packet to the destination network. An entry of two colons (::) indicates that the router has some non-BGP routes to this network.
Metric	If shown, this is the value of the interautonomous system metric.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

The following is sample output from the **show bgp ipv6** command, showing information for prefix 3FFE:500::/24:

```
Router# show bgp ipv6 unicast 3FFE:500::/24

BGP routing table entry for 3FFE:500::/24, version 19421
Paths: (6 available, best #1)
  Advertised to peer-groups:
     6BONE
  293 3425 2500
    3FFE:700:20:1::11 from 3FFE:700:20:1::11 (192.168.2.27)
      Origin IGP, localpref 100, valid, external, best
  4554 293 3425 2500
    3FFE:C00:E:4::2 from 3FFE:C00:E:4::2 (192.168.1.1)
      Origin IGP, metric 1, localpref 100, valid, external
  33 293 3425 2500
    3FFE:C00:E:5::2 from 3FFE:C00:E:5::2 (209.165.18.254)
      Origin IGP, localpref 100, valid, external
      Dampinfo: penalty 673, flapped 429 times in 10:47:45
  6175 7580 2500
    3FFE:C00:E:1::2 from 3FFE:C00:E:1::2 (209.165.223.204)
      Origin IGP, localpref 100, valid, external
1849 4697 2500, (suppressed due to dampening)
    3FFE:1100:0:CC00::1 from 3FFE:1100:0:CC00::1 (172.31.38.102)
      Origin IGP, localpref 100, valid, external
      Dampinfo: penalty 3938, flapped 596 times in 13:03:06, reuse in 00:59:10
237 10566 4697 2500
    3FFE:C00:E:B::2 from 3FFE:C00:E:B::2 (172.31.0.3)
      Origin IGP, localpref 100, valid, external
```

The following is sample output from the **show bgp ipv6** command, showing MPLS label information for an IPv6 prefix that is configured to be an IPv6 edge router using MPLS:

```
Router# show bgp ipv6 unicast 2001:0DB8::/32

BGP routing table entry for 2001:0DB8::/32, version 15
Paths: (1 available, best #1)
  Not advertised to any peer
  Local
    ::FFFF:192.168.99.70 (metric 20) from 192.168.99.70 (192.168.99.70)
      Origin IGP, localpref 100, valid, internal, best, mpls label 17
```

To display the top of the stack label with label switching information, enter the **show bgp ipv6** EXEC command with the **labels** keyword:

```
Router# show bgp ipv6 unicast labels

Network              Next Hop               In tag/Out tag
2001:0DB8::/32       ::FFFF:192.168.99.70   notag/20
```

Note If a prefix has not been advertised to any peer, the display shows "Not advertised to any peer."

The following is sample output from the **show bgp ipv6** command, showing 6PE multipath information. The prefix 4004::/64 is received by BGP from two different peers and therefore two different paths:

```
Router# show bgp ipv6 unicast

BGP table version is 28, local router ID is 172.10.10.1
Status codes:s suppressed, d damped, h history, * valid, > best, i -
internal,
              r RIB-failure, S Stale
Origin codes:i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path

*>i4004::/64        ::FFFF:172.11.11.1
                                             0    100      0 ?
* i                 ::FFFF:172.30.30.1
                                             0    100      0 ?
```

Related Commands

Command	Description
clear bgp ipv6	Resets an IPv6 BGP connection or session.
neighbor soft-reconfiguration	Configures the Cisco IOS software to start storing updates.

show bgp ipv6 community

To display routes that belong to specified IPv6 Border Gateway Protocol (BGP) communities, use the **show bgp ipv6 community** command in user EXEC or privileged EXEC mode.

show bgp ipv6 {**unicast** | **multicast**} **community** [*community-number*] [**exact-match**] [**local-as** | **no-advertise** | **no-export**]

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.
community-number	(Optional) Valid value is a community number in the range from 1 to 4294967295 or AA:NN (autonomous system-community number:2-byte number).
exact-match	(Optional) Displays only routes that have an exact match.
local-as	(Optional) Displays only routes that are not sent outside of the local autonomous system (well-known community).
no-advertise	(Optional) Displays only routes that are not advertised to any peer (well-known community).
no-export	(Optional) Displays only routes that are not exported outside of the local autonomous system (well-known community).

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(2)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 Release 12.2(14)S.
12.3(2)T	The **unicast** and **exact-match** keywords were added.
12.0(26)S	The **unicast** and **multicast** keywords were added.
12.3(4)T	The **multicast** keyword was 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.
12.2(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 bgp ipv6 community** command provides output similar to the **show ip bgp community** command, except it is IPv6-specific.

Communities are set with the **set community** route-map configuration command. You must enter the numerical communities before the well-known communities. For example, the following string is not valid:

```
Router# show ipv6 bgp community local-as 111:12345
```

Use one of the following strings instead:

```
Router# show ipv6 bgp community 111:12345 local-as

Router# show ipv6 bgp unicast community 111:12345 local-as
```

The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the **unicast** keyword is mandatory starting with Cisco IOS Release 12.3(2)T.

The **multicast** keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

The following is sample output from the **show bgp ipv6 community** command:

Note The output is the same whether or not the **unicast** or **multicast** keyword is used. The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and Cisco IOS Release 12.0(26)S and later releases, and the **multicast** keyword is available only in Cisco IOS Release 12.0(26)S and later releases.

```
BGP table version is 69, local router ID is 10.2.64.5
Status codes:s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes:i - IGP, e - EGP, ? - incomplete

      Network               Next Hop              Metric LocPrf Weight Path
*> 2001:0DB8:0:1::1/64       ::                                   0 32768 i
*> 2001:0DB8:0:1:1::/80      ::                                   0 32768 ?
*> 2001:0DB8:0:2::/64        2001:0DB8:0:3::2                        0 2 i
*> 2001:0DB8:0:2:1::/80      2001:0DB8:0:3::2                        0 2 ?
* 2001:0DB8:0:3::1/64        2001:0DB8:0:3::2                        0 2 ?
*>                        ::                                  0 32768 ?
*> 2001:0DB8:0:4::/64        2001:0DB8:0:3::2                        0 2 ?
*> 2001:0DB8:0:5::1/64       ::                                   0 32768 ?
*> 2001:0DB8:0:6::/64        2000:0:0:3::2                        0 2 3 i
*> 2010::/64                 ::                                   0 32768 ?
*> 2020::/64                 ::                                   0 32768 ?
*> 2030::/64                 ::                                   0 32768 ?
*> 2040::/64                 ::                                   0 32768 ?
*> 2050::/64                 ::                                   0 32768 ?
```

Table 58 describes the significant fields shown in the display.

Table 58 show bgp ipv6 community Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	A 32-bit number written as 4 octets separated by periods (dotted-decimal format).

Table 58 show bgp ipv6 community Field Descriptions (continued)

Field	Description
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. d—The table entry is dampened. h—The table entry is history. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP session.
Origin codes	Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from the Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. e—Entry originated from the Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IPv6 address of a network entity.
Next Hop	IPv6 address of the next system that is used when forwarding a packet to the destination network. An entry of two colons (::) indicates that the router has some non-BGP routes to this network.
Metric	The value of the interautonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

Related Commands

Command	Description
clear bgp ipv6	Resets an IPv6 BGP connection or session.
ip bgp-community new-format	Displays BGP communities in the format AA:NN (autonomous system-community number:2-byte number).
neighbor soft-reconfiguration	Configures the Cisco IOS software to start storing updates.

show bgp ipv6 community-list

To display routes that are permitted by the IPv6 Border Gateway Protocol (BGP) community list, use the **show bgp ipv6 community-list** command in user EXEC or privileged EXEC mode.

show bgp ipv6 {**unicast** | **multicast**} **community-list** {*number* | *name*} [**exact-match**]

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.
number	Community list number in the range from 1 to 199.
name	Community list name.
exact-match	(Optional) Displays only routes that have an exact match.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(2)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 Release 12.2(14)S.
12.3(2)T	The **unicast** keyword was added.
12.0(26)S	The **unicast** and **multicast** keywords were added.
12.3(4)T	The **multicast** keyword was 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.
12.2(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 bgp ipv6 unicast community-list** and **show bgp ipv6 multicast community-list** commands provide output similar to the **show ip bgp community-list** command, except they are IPv6-specific.

The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the **unicast** keyword is mandatory starting with Cisco IOS Release 12.3(2)T.

The **multicast** keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

The following is sample output of the **show bgp ipv6 community-list** command for community list number 3:

Note The output is the same whether or not the **unicast** or **multicast** keyword is used. The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and Cisco IOS Release 12.0(26)S and later releases, and the **multicast** keyword is available only in Cisco IOS Release 12.0(26)S and later releases.

```
Router# show bgp ipv6 unicast community-list 3

BGP table version is 14, local router ID is 10.2.64.6
Status codes:s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes:i - IGP, e - EGP, ? - incomplete

    Network                Next Hop            Metric LocPrf Weight Path
*> 2001:0DB8:0:1::/64     2001:0DB8:0:3::1                         0 1 i
*> 2001:0DB8:0:1:1::/80   2001:0DB8:0:3::1                         0 1 i
*> 2001:0DB8:0:2::1/64    ::                                     0 32768 i
*> 2001:0DB8:0:2:1::/80   ::                                     0 32768 ?
* 2001:0DB8:0:3::2/64     2001:0DB8:0:3::1                         0 1 ?
*>                       ::                                   0 32768 ?
*> 2001:0DB8:0:4::2/64    ::                                     0 32768 ?
*> 2001:0DB8:0:5::/64     2001:0DB8:0:3::1                         0 1 ?
*> 2010::/64              2001:0DB8:0:3::1                         0 1 ?
*> 2020::/64              2001:0DB8:0:3::1                         0 1 ?
*> 2030::/64              2001:0DB8:0:3::1                         0 1 ?
*> 2040::/64              2001:0DB8:0:3::1                         0 1 ?
*> 2050::/64              2001:0DB8:0:3::1                         0 1 ?
```

Table 59 describes the significant fields shown in the display.

Table 59 show bgp ipv6 community-list Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	A 32-bit number written as 4 octets separated by periods (dotted-decimal format).
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s—The table entry is suppressed. • d—The table entry is dampened. • h—The table entry is history. • *—The table entry is valid. • >—The table entry is the best entry to use for that network. • i—The table entry was learned via an internal BGP session.

Table 59 show bgp ipv6 community-list Field Descriptions (continued)

Field	Description
Origin codes	Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: • i—Entry originated from the Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • e—Entry originated from the Exterior Gateway Protocol (EGP). • ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IPv6 address of a network entity.
Next Hop	IPv6 address of the next system that is used when forwarding a packet to the destination network. An entry of two colons (::) indicates that the router has some non-BGP routes to this network.
Metric	The value of the interautonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

Related Commands

Command	Description
clear bgp ipv6	Resets an IPv6 BGP connection or session.
neighbor soft-reconfiguration	Configures the Cisco IOS software to start storing updates.

show bgp ipv6 dampened-paths

To display IPv6 Border Gateway Protocol (BGP) dampened routes, use the **show bgp ipv6 dampened-paths** command in user EXEC or privileged EXEC mode.

show bgp ipv6 {**unicast** | **multicast**} **dampening dampened-paths**

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.
dampening	Displays detailed information about dampening.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(2)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 Release 12.2(14)S.
12.3(2)T	The **unicast** and **dampening** keywords were added.
12.0(26)S	The **unicast** and **multicast** keywords were added.
12.3(4)T	The **multicast** keyword was 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.
12.2(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 introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The **show bgp ipv6 dampened-paths** and **show bgp ipv6 unicast dampening dampened-paths** commands provide output similar to the **show ip bgp dampened-paths** command, except they are IPv6-specific.

The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the **unicast** keyword is mandatory starting with Cisco IOS Release 12.3(2)T.

The **multicast** keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

The following is sample output from the **show bgp ipv6 dampened-paths** command:

Note The command output is the same whether or not the **unicast, multicast,** and **dampening** keywords are used. The **unicast** and **dampening** keywords are available only in Cisco IOS Release 12.3(2)T and Cisco IOS Release 12.0(26)S and later releases, and the **multicast** keyword is available only in Cisco IOS Release 12.0(26)S and later releases.

```
Router# show bgp ipv6 unicast dampening dampened-paths

BGP table version is 12610, local router ID is 192.168.7.225
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          From             Reuse    Path
*d 3FFE:1000::/24   3FFE:C00:E:B::2  00:00:10 237 2839 5609 i
*d 2001:228::/35    3FFE:C00:E:B::2  00:23:30 237 2839 5609 2713 i
```

Table 60 describes the significant fields shown in the display.

Table 60 show bgp ipv6 dampened-paths Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	A 32-bit number written as 4 octets separated by periods (dotted-decimal format).
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. d—The table entry is dampened. h—The table entry is history. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP session.
Origin codes	Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from the Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. e—Entry originated from the Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear Usually, this is a router that is redistributed into BGP from an IGP.
Network	Indicates the network to which the route is dampened.
From	IPv6 address of the peer that advertised this path.
Reuse	Time (in hours:minutes:seconds) after which the path will be made available.
Path	Autonomous system path of the route that is being dampened.

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes various BGP route dampening factors.
clear bgp ipv6 dampening	Clears IPv6 BGP route dampening information and unsuppresses the suppressed routes.

show bgp ipv6 filter-list

To display routes that conform to a specified IPv6 filter list, use the **show bgp ipv6 filter-list** command in user EXEC or privileged EXEC mode.

show bgp ipv6 {**unicast** | **multicast**} **filter-list** *access-list-number*

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.
access-list-number	Number of an IPv6 autonomous system path access list. It can be a number from 1 to 199.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(2)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 Release 12.2(14)S.
12.3(2)T	The **unicast** keyword was added.
12.0(26)S	The **unicast** and **multicast** keywords were added.
12.3(4)T	The **multicast** keyword was 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.
12.2(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 bgp ipv6 filter-list** command provides output similar to the **show ip bgp filter-list** command, except that it is IPv6-specific.

The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the **unicast** keyword is mandatory starting with Cisco IOS Release 12.3(2)T.

The **multicast** keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

The following is sample output from the **show bgp ipv6 filter-list** command for IPv6 autonomous system path access list number 1:

Note The output is the same whether or not the **unicast** or **multicast** keyword is used. The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and Cisco IOS Release 12.0(26)S and later releases, and the **multicast** keyword is available only in Cisco IOS Release 12.0(26)S and later releases.

```
Router# show bgp ipv6 unicast filter-list 1

BGP table version is 26, local router ID is 192.168.0.2
Status codes:s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes:i - IGP, e - EGP, ? - incomplete

    Network              Next Hop                            Metric LocPrf Weight Path
*> 2001:0DB8:0:1::/64        2001:0DB8:0:4::2                         0 2 1 i
*> 2001:0DB8:0:1:1::/80      2001:0DB8:0:4::2                         0 2 1 i
*> 2001:0DB8:0:2:1::/80      2001:0DB8:0:4::2                         0 2 ?
*> 2001:0DB8:0:3::/64        2001:0DB8:0:4::2                         0 2 ?
*> 2001:0DB8:0:4::/64        ::                                         32768  ?
*                            2001:0DB8:0:4::2                         0 2 ?
*> 2001:0DB8:0:5::/64        ::                                         32768  ?
*                            2001:0DB8:0:4::2                         0 2 1 ?
*> 2001:0DB8:0:6::1/64       ::                                         32768  i
*> 2030::/64                 2001:0DB8:0:4::2                         0 1
*> 2040::/64                 2001:0DB8:0:4::2                         0 2 1 ?
*> 2050::/64                 2001:0DB8:0:4::2                         0 2 1 ?
```

Table 61 describes the significant fields shown in the display.

Table 61 show bgp ipv6 filter-list Field Descriptions

Field	Description
BGP table version	Internal version number for the table. This number is incremented any time the table changes.
local router ID	A 32-bit number written as 4 octets separated by periods (dotted-decimal format).
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s—The table entry is suppressed. • d—The table entry is dampened. • h—The table entry is history. • *—The table entry is valid. • >—The table entry is the best entry to use for that network. • i—The table entry was learned via an internal BGP session.
Origin codes	Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: • i—Entry originated from Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • e—Entry originated from Exterior Gateway Protocol (EGP). • ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IPv6 address of the network the entry describes.

Table 61 show bgp ipv6 filter-list Field Descriptions (continued)

Field	Description
Next Hop	IPv6 address of the next system that is used when forwarding a packet to the destination network. An entry of two colons (::) indicates that the router has some non-BGP routes to this network.
Metric	If shown, this is the value of the interautonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path. At the end of the path is the origin code for the path. It can be one of the following values: • i—The entry was originated with the IGP and advertised with a **network** router configuration command. • e—The route originated with EGP. • ?—The origin of the path is not clear. Usually this is a path that is redistributed into BGP from an IGP.

Related Commands

Command	Description
ip as-path access-list	Defines a BGP autonomous system path access list.

show bgp ipv6 flap-statistics

To display IPv6 Border Gateway Protocol (BGP) flap statistics, use the **show bgp ipv6 flap-statistics** command in user EXEC or privileged EXEC mode.

show bgp ipv6 {**unicast** | **multicast**} **dampening flap-statistics** [**regexp** *regular-expression* | **quote-regexp** *regular-expression* | **filter-list** *list* | *ipv6-prefix*/*prefix-length* [**longer-prefix**]]

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.
dampening	Displays detailed information about dampening.
regexp *regular-expression*	(Optional) Displays flap statistics for all the paths that match the regular expression.
quote-regexp *regular-expression*	(Optional) Displays flap statistics for all the paths that match the regular expression as a quoted string of characters.
filter-list *list*	(Optional) Displays flap statistics for all the paths that pass the access list.
ipv6-prefix	(Optional) Displays flap statistics for a single entry at this IPv6 network number. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/prefix-length	(Optional) The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
longer-prefix	(Optional) Displays flap statistics for more specific entries.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(2)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 Release 12.2(14)S.
12.3(2)T	The **unicast** and **dampening** keywords were added.
12.0(26)S	The **unicast** and **multicast** keywords were added.
12.3(4)T	The **unicast** and **multicast** keywords 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.
12.2(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 bgp ipv6 unicast dampening flap-statistics** and **show bgp ipv6 multicast dampening flap-statistics** commands provide output similar to the **show ip bgp flap-statistics** command, except they are IPv6-specific.

If no arguments or keywords are specified, the router displays flap statistics for all routes.

The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the **unicast** keyword is mandatory starting with Cisco IOS Release 12.3(2)T.

The **multicast** keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

The following is sample output from the **show bgp ipv6 flap-statistics** command without arguments or keywords:

Note The output is the same whether or not the **unicast, multicast,** and **dampening** keywords are used. The **unicast** and **dampening** keywords are available only in Cisco IOS Release 12.3(2)T and Cisco IOS Release 12.0(26)S and later releases, and the **multicast** keyword is available only in Cisco IOS Release 12.0(26)S and later releases.

```
Router# show bgp ipv6 unicast dampening flap-statistics

BGP table version is 12612, local router ID is 192.168.7.225
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          From            Flaps Duration Reuse    Path
*d 2001:200::/35    3FFE:1100:0:CC00::1
                                    12145 10:09:15 00:57:10 1849 2914 4697 2500
*  2001:218::/35    2001:0DB8:0:F004::1
                                    2     00:03:44          3462 4697
```

Table 62 describes the significant fields shown in the display.

Table 62 show bgp ipv6 flap-statistics Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	A 32-bit number written as 4 octets separated by periods (dotted-decimal format).

Table 62 show bgp ipv6 flap-statistics Field Descriptions (continued)

Field	Description
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s—The table entry is suppressed. • d—The table entry is dampened. • h—The table entry is history. • *—The table entry is valid. • >—The table entry is the best entry to use for that network. • i—The table entry was learned via an internal BGP session.
Origin codes	Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: • i—Entry originated from the Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • e—Entry originated from the Exterior Gateway Protocol (EGP). • ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	Route to the network indicated is dampened.
From	IPv6 address of the peer that advertised this path.
Flaps	Number of times the route has flapped.
Duration	Time (hours:minutes:seconds) since the router noticed the first flap.
Reuse	Time (in hours:minutes:seconds) after which the path will be made available.
Path	Autonomous system path of the route that is being dampened.

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes various BGP route dampening factors.
clear bgp ipv6 flap-statistics	Clears IPv6 BGP flap statistics.
ip as-path access-list	Defines a BGP autonomous system path access list.

show bgp ipv6 inconsistent-as

To display IPv6 Border Gateway Protocol (BGP) routes with inconsistent originating autonomous systems, use the **show bgp ipv6 inconsistent-as** command in user EXEC or privileged EXEC mode.

show bgp ipv6 {**unicast** | **multicast**} **inconsistent-as**

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(2)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 Release 12.2(14)S.
12.3(2)T	The **unicast** keyword was added.
12.0(26)S	The **unicast** and **multicast** keywords were added.
12.3(4)T	The **multicast** keyword was 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.
12.2(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 bgp ipv6 unicast inconsistent-as** and **show bgp ipv6 multicast inconsistent-as** commands provide output similar to the **show ip bgp inconsistent-as** command, except they are IPv6-specific.

The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the **unicast** keyword is mandatory starting with Cisco IOS Release 12.3(2)T.

The **multicast** keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

The following is sample output from the **show bgp ipv6 inconsistent-as** command:

Note The output is the same whether or not the **unicast** or **multicast** keyword is used. The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and Cisco IOS Release 12.0(26)S and later releases, and the **multicast** keyword is available only in Cisco IOS Release 12.0(26)S and later releases.

```
Router# show bgp ipv6 unicast inconsistent-as

BGP table version is 12612, local router ID is 192.168.7.225
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*  3FFE:1300::/24   2001:0DB8:0:F004::1                    0 3320 293 6175 ?
*                   3FFE:C00:E:9::2                       0 1251 4270 10318 ?
*                   3FFE:3600::A                          0 3462 6175 ?
*                   3FFE:700:20:1::11                     0 293 6175 ?
```

Table 63 describes the significant fields shown in the display.

Table 63 show bgp ipv6 inconsistent-as Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	A 32-bit number written as 4 octets separated by periods (dotted decimal format).
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s—The table entry is suppressed. • d—The table entry is dampened. • h—The table entry is history. • *—The table entry is valid. • >—The table entry is the best entry to use for that network. • i—The table entry was learned via an internal BGP session.
Origin codes	Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: • i—Entry originated from the Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • e—Entry originated from the Exterior Gateway Protocol (EGP). • ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IPv6 address of the network the entry describes.
Next Hop	IPv6 address of the next system that is used when forwarding a packet to the destination network. An entry of two colons (::) indicates that the router has some non-BGP routes to this network.
Metric	The value of the interautonomous system metric. This field is frequently not used.

Table 63 show bgp ipv6 inconsistent-as Field Descriptions (continued)

Field	Description
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

show bgp ipv6 labels

To display the status of all IPv6 Border Gateway Protocol (BGP) connections, use the **show bgp ipv6 labels** command in user EXEC or privileged EXEC mode.

show bgp ipv6 {**unicast** | **multicast**} **labels**

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.0(26)S	The **unicast** and **multicast** keywords were added.
12.3(4)T	The **unicast** and **multicast** keywords were added.

Usage Guidelines

The **multicast** keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

The following is sample output from the **show bgp ipv6 labels** command:

Note The output is the same whether or not the **unicast** or **multicast** keyword is used. The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and Cisco IOS Release 12.0(26)S and later releases, and the **multicast** keyword is available only in Cisco IOS Release 12.0(26)S and later releases.

```
Router# show bgp ipv6 unicast labels

Network                    Next Hop        In label/Out label
2001:1:101::1/128          ::FFFF:172.17.1.1  nolabel/19
2001:3:101::1/128          ::FFFF:172.25.8.8  nolabel/19
```

Table 64 describes the significant fields shown in the display.

Table 64 show bgp ipv6 labels Field Descriptions

Field	Description
Network	IPv6 address of the network the entry describes.

Table 64 show bgp ipv6 labels Field Descriptions (continued)

Field	Description
Next Hop	IPv6 address of the next system that is used when forwarding a packet to the destination network. An entry of two colons (::) indicates that the router has some non-BGP routes to this network.
In label/Out label	IPv6 BGP connections.

show bgp ipv6 neighbors

To display information about IPv6 Border Gateway Protocol (BGP) connections to neighbors, use the **show bgp ipv6 neighbors** command in user EXEC or privileged EXEC mode.

show bgp ipv6 {**unicast** | **multicast**} **neighbors** [*ipv6-address*] [**received-routes** | **routes** | **flap-statistics** | **advertised-routes** | **paths** *regular-expression* | **dampened-routes**]

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.
ipv6-address	(Optional) Address of the IPv6 BGP-speaking neighbor. If you omit this argument, all IPv6 neighbors are displayed. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
received-routes	(Optional) Displays all received routes (both accepted and rejected) from the specified neighbor.
routes	(Optional) Displays all routes received and accepted. This is a subset of the output from the **received-routes** keyword.
flap-statistics	(Optional) Displays flap statistics for the routes learned from the neighbor.
advertised-routes	(Optional) Displays all the routes the networking device advertised to the neighbor.
paths *regular-expression*	(Optional) Regular expression used to match the paths received.
dampened-routes	(Optional) Displays the dampened routes to the neighbor at the IP address specified.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(2)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	IPv6 capability information was added to the display.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(2)T	The **unicast** keyword was added.
12.0(26)S	The **unicast** and **multicast** keywords were added.
12.3(4)T	The **multicast** keyword was 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.
12.2(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 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

The **show bgp ipv6 unicast neighbors** and **show bgp ipv6 multicast neighbors** commands provide output similar to the **show ip bgp neighbors** command, except they are IPv6-specific.

The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the **unicast** keyword is mandatory starting with Cisco IOS Release 12.3(2)T.

The **multicast** keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

The following is sample output from the **show bgp ipv6 neighbors** command:

Note The output is the same whether or not the **unicast** or **multicast** keyword is used. The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and Cisco IOS Release 12.0(26)S and later releases, and the **multicast** keyword is available only in Cisco IOS Release 12.0(26)S and later releases.

```
Router# show bgp ipv6 unicast neighbors

BGP neighbor is 3FFE:700:20:1::11,  remote AS 65003, external link
 Member of peer-group 6BONE for session parameters
  BGP version 4, remote router ID 192.168.2.27
  BGP state = Established, up for 13:40:17
  Last read 00:00:09, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received
    Address family IPv6 Unicast: advertised and received
  Received 31306 messages, 20 notifications, 0 in queue
  Sent 14298 messages, 1 notifications, 0 in queue
  Default minimum time between advertisement runs is 30 seconds

 For address family: IPv6 Unicast
  BGP table version 21880, neighbor version 21880
  Index 1, Offset 0, Mask 0x2
  Route refresh request: received 0, sent 0
  6BONE peer-group member
  Community attribute sent to this neighbor
  Outbound path policy configured
  Incoming update prefix filter list is bgp-in
  Outgoing update prefix filter list is aggregate
  Route map for outgoing advertisements is uni-out
  77 accepted prefixes consume 4928 bytes
  Prefix advertised 4303, suppressed 0, withdrawn 1328
  Number of NLRIs in the update sent: max 1, min 0
  1 history paths consume 64 bytes

  Connections established 22; dropped 21
  Last reset 13:47:05, due to BGP Notification sent, hold time expired
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Local host: 3FFE:700:20:1::12, Local port: 55345
Foreign host: 3FFE:700:20:1::11, Foreign port: 179

Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)

Event Timers (current time is 0x1A0D543C):
Timer          Starts    Wakeups            Next
Retrans          1218          5             0x0
TimeWait            0          0             0x0
```

```
AckHold          3327       3051             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0

iss: 1805423033  snduna: 1805489354  sndnxt: 1805489354     sndwnd:  15531
irs:  821333727  rcvnxt:  821591465  rcvwnd:      15547  delrcvwnd:    837

SRTT: 300 ms, RTTO: 303 ms, RTV: 3 ms, KRTT: 0 ms
minRTT: 8 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: higher precedence, nagle

Datagrams (max data segment is 1420 bytes):
Rcvd: 4252 (out of order: 0), with data: 3328, total data bytes: 257737
Sent: 4445 (retransmit: 5), with data: 4445, total data bytes: 244128
```

The following is sample output from the **show bgp ipv6 neighbors** command when the router is configured to allow IPv6 traffic to be transported across an IPv4 Multiprotocol Label Switching (MPLS) network (Cisco 6PE) without any software or hardware upgrade in the IPv4 core infrastructure. A new neighbor capability is added to show that an MPLS label is assigned for each IPv6 address prefix to be advertised. 6PE uses multiprotocol BGP to provide the reachability information for the 6PE routers across the IPv4 network so that the neighbor addresses are IPv4.

```
Router# show bgp ipv6 unicast neighbors

BGP neighbor is 10.11.11.1,  remote AS 65000, internal link
  BGP version 4, remote router ID 10.11.11.1
  BGP state = Established, up for 04:00:53
  Last read 00:00:02, hold time is 15, keepalive interval is 5 seconds
  Configured hold time is 15, keepalive interval is 10 seconds
  Neighbor capabilities:
    Route refresh: advertised and received(old & new)
    Address family IPv6 Unicast: advertised and received
    ipv6 MPLS Label capability: advertised and received
  Received 67068 messages, 1 notifications, 0 in queue
  Sent 67110 messages, 16 notifications, 0 in queue
  Default minimum time between advertisement runs is 5 seconds

 For address family: IPv6 Unicast
  BGP table version 91, neighbor version 91
  Index 1, Offset 0, Mask 0x2
  Route refresh request: received 0, sent 0
  Sending Prefix & Label
  4 accepted prefixes consume 288 bytes
  Prefix advertised 90, suppressed 0, withdrawn 2
  Number of NLRIs in the update sent: max 3, min 0

  Connections established 26; dropped 25
  Last reset 04:01:20, due to BGP Notification sent, hold time expired
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Local host: 10.10.10.1, Local port: 179
Foreign host: 10.11.11.1, Foreign port: 11003

Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)

Event Timers (current time is 0x1429F084):
Timer          Starts    Wakeups            Next
Retrans          2971         77             0x0
TimeWait            0          0             0x0
AckHold          2894       1503             0x0
SendWnd             0          0             0x0
```

```
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0

iss:  803218558  snduna:  803273755  sndnxt:  803273755     sndwnd:  16289
irs: 4123967590  rcvnxt: 4124022787  rcvwnd:      16289  delrcvwnd:     95

SRTT: 300 ms, RTTO: 303 ms, RTV: 3 ms, KRTT: 0 ms
minRTT: 32 ms, maxRTT: 408 ms, ACK hold: 200 ms
Flags: passive open, nagle, gen tcbs

Datagrams (max data segment is 536 bytes):
Rcvd: 4531 (out of order: 0), with data: 2895, total data bytes: 55215
Sent: 4577 (retransmit: 77, fastretransmit: 0), with data: 2894, total data
bytes: 55215
```

Table 119 describes the significant fields shown in the display.

Table 119 show bgp ipv6 neighbors Field Descriptions

Field	Description
BGP neighbor	IP address of the BGP neighbor and its autonomous system number. If the neighbor is in the same autonomous system as the router, then the link between them is internal; otherwise, it is considered external.
remote AS	Autonomous system of the neighbor.
internal link	Indicates that this peer is an interior Border Gateway Protocol (iBGP) peer.
BGP version	BGP version being used to communicate with the remote router; the router ID (an IP address) of the neighbor is also specified.
remote router ID	A 32-bit number written as 4 octets separated by periods (dotted-decimal format).
BGP state	Internal state of this BGP connection.
up for	Amount of time that the underlying TCP connection has been in existence.
Last read	Time that BGP last read a message from this neighbor.
hold time	Maximum amount of time that can elapse between messages from the peer.
keepalive interval	Time period between sending keepalive packets, which help ensure that the TCP connection is up.
Neighbor capabilities	BGP capabilities advertised and received from this neighbor.
Route refresh	Indicates that the neighbor supports dynamic soft reset using the route refresh capability.
Address family IPv6 Unicast	Indicates that BGP peers are exchanging IPv6 reachability information.
ipv6 MPLS Label capability	Indicates that MPLS labels are being assigned to IPv6 address prefixes.
Received	Number of total BGP messages received from this peer, including keepalives.
notifications	Number of error messages received from the peer.
Sent	Total number of BGP messages that have been sent to this peer, including keepalives.
notifications	Number of error messages the router has sent to this peer.

Table 119 show bgp ipv6 neighbors Field Descriptions (continued)

Field	Description
advertisement runs	Value of the minimum advertisement interval.
For address family	Address family to which the following fields refer.
BGP table version	Indicates that the neighbor has been updated with this version of the primary BGP routing table.
neighbor version	Number used by the software to track the prefixes that have been sent and those that must be sent to this neighbor.
Route refresh request	Number of route refresh requests sent and received from this neighbor.
Community attribute (not shown in sample output)	Appears if the **neighbor send-community** command is configured for this neighbor.
Inbound path policy (not shown in sample output)	Indicates whether an inbound filter list or route map is configured.
Outbound path policy (not shown in sample output)	Indicates whether an outbound filter list, route map, or unsuppress map is configured.
bgp-in (not shown in sample output)	Name of the inbound update prefix filter list for the IPv6 unicast address family.
aggregate (not shown in sample output)	Name of the outbound update prefix filter list for the IPv6 unicast address family.
uni-out (not shown in sample output)	Name of the outbound route map for the IPv6 unicast address family.
accepted prefixes	Number of prefixes accepted.
Prefix advertised	Number of prefixes advertised.
suppressed	Number of prefixes suppressed.
withdrawn	Number of prefixes withdrawn.
history paths (not shown in sample output)	Number of path entries held to remember history.
Connections established	Number of times the router has established a TCP connection and the two peers have agreed to speak BGP with each other.
dropped	Number of times that a good connection has failed or been taken down.
Last reset	Elapsed time (in hours:minutes:seconds) since this peering session was last reset.
Connection state	State of the BGP peer.
unread input bytes	Number of bytes of packets still to be processed.
Local host, Local port	Peering address of the local router, plus the port.
Foreign host, Foreign port	Peering address of the neighbor.
Event Timers	Table that displays the number of starts and wakeups for each timer.

Table 119 show bgp ipv6 neighbors Field Descriptions (continued)

Field	Description
iss	Initial send sequence number.
snduna	Last send sequence number for which the local host sent but has not received an acknowledgment.
sndnxt	Sequence number the local host will send next.
sndwnd	TCP window size of the remote host.
irs	Initial receive sequence number.
rcvnxt	Last receive sequence number the local host has acknowledged.
rcvwnd	TCP window size of the local host.
delrecvwnd	Delayed receive window—data the local host has read from the connection, but has not yet subtracted from the receive window the host has advertised to the remote host. The value in this field gradually increases until it is larger than a full-sized packet, at which point it is applied to the rcvwnd field.
SRTT	A calculated smoothed round-trip timeout (in milliseconds).
RTTO	Round-trip timeout (in milliseconds).
RTV	Variance of the round-trip time (in milliseconds).
KRTT	New round-trip timeout (in milliseconds) using the Karn algorithm. This field separately tracks the round-trip time of packets that have been re-sent.
minRTT	Smallest recorded round-trip timeout (in milliseconds) with hard wire value used for calculation.
maxRTT	Largest recorded round-trip timeout (in milliseconds).
ACK hold	Time (in milliseconds) the local host will delay an acknowledgment in order to “piggyback” data on it.
Flags	IP precedence of the BGP packets.
Datagrams: Rcvd	Number of update packets received from neighbor.
with data	Number of update packets received with data.
total data bytes	Total number of bytes of data.
Sent	Number of update packets sent.
with data	Number of update packets with data sent.
total data bytes	Total number of data bytes.

The following is sample output from the **show bgp ipv6 neighbors** command with the **advertised-routes** keyword:

```
Router# show bgp ipv6 unicast neighbors 3FFE:700:20:1::11 advertised-routes

BGP table version is 21880, local router ID is 192.168.7.225
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 2001:200::/35    3FFE:700:20:1::11                      0 293 3425 2500 i
*> 2001:208::/35    3FFE:C00:E:B::2                        0 237 7610 i
*> 2001:218::/35    3FFE:C00:E:C::2                        0 3748 4697 i
```

The following is sample output from the **show bgp ipv6 neighbors** command with the **routes** keyword:

```
Router# show bgp ipv6 unicast neighbors 3FFE:700:20:1::11 routes

BGP table version is 21885, local router ID is 192.168.7.225
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 2001:200::/35    3FFE:700:20:1::11                       0 293 3425 2500 i
*  2001:208::/35    3FFE:700:20:1::11                       0 293 7610 i
*  2001:218::/35    3FFE:700:20:1::11                       0 293 3425 4697 i
*  2001:230::/35    3FFE:700:20:1::11                       0 293 1275 3748 i
```

Table 120 describes the significant fields shown in the display.

Table 120 show bgp ipv6 neighbors advertised-routes and routes Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	A 32-bit number written as 4 octets separated by periods (dotted-decimal format).
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s—The table entry is suppressed. • d—The table entry is dampened. • h—The table entry is history. • *—The table entry is valid. • >—The table entry is the best entry to use for that network. • i—The table entry was learned via an internal BGP session.
Origin codes	Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: • i—Entry originated from the Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • e—Entry originated from the Exterior Gateway Protocol (EGP). • ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IPv6 address of the network the entry describes.
Next Hop	IPv6 address of the next system that is used when forwarding a packet to the destination network. An entry of two colons (::) indicates that the router has some non-BGP routes to this network.
Metric	The value of the interautonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.

Table 120 show bgp ipv6 neighbors advertised-routes and routes Field Descriptions (continued)

Field	Description
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

The following is sample output from the **show bgp ipv6 neighbors** command with the **paths** keyword:

```
Router# show bgp ipv6 unicast neighbors 3FFE:700:20:1::11 paths ^293

Address    Refcount Metric Path
0x6131D7DC        2      0 293 3425 2500 i
0x6132861C        2      0 293 7610 i
0x6131AD18        2      0 293 3425 4697 i
0x61324084        2      0 293 1275 3748 i
0x61320E0C        1      0 293 3425 2500 2497 i
0x61326928        1      0 293 3425 2513 i
0x61327BC0        2      0 293 i
0x61321758        1      0 293 145 i
0x61320BEC        1      0 293 3425 6509 i
0x6131AAF8        2      0 293 1849 2914 ?
0x61320FE8        1      0 293 1849 1273 209 i
0x613260A8        2      0 293 1849 i
0x6132586C        1      0 293 1849 5539 i
0x6131BBF8        2      0 293 1849 1103 i
0x6132344C        1      0 293 4554 1103 1849 1752 i
0x61324150        2      0 293 1275 559 i
0x6131E5AC        2      0 293 1849 786 i
0x613235E4        1      0 293 1849 1273 i
0x6131D028        1      0 293 4554 5539 8627 i
0x613279E4        1      0 293 1275 3748 4697 3257 i
0x61320328        1      0 293 1849 1273 790 i
0x6131EC0C        2      0 293 1275 5409 i
```

Note The caret (^) symbol in the example is a regular expression that is entered by simultaneously pressing the Shift and 6 keys on your keyboard. A caret (^) symbol at the beginning of a regular expression matches the start of a line.

Table 121 describes the significant fields shown in the display.

Table 121 show bgp ipv6 neighbors paths Field Descriptions

Field	Description
Address	Internal address where the path is stored.
Refcount	Number of routes using that path.
Metric	The Multi Exit Discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.)
Path	The autonomous system path for that route, followed by the origin code for that route.

The following sample output from the **show bgp ipv6 neighbors** command shows the dampened routes for IPv6 address 3FFE:700:20:1::11:

```
Router# show bgp ipv6 unicast neighbors 3FFE:700:20:1::11 dampened-routes
```

```
BGP table version is 32084, local router ID is 192.168.7.225
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          From             Reuse    Path
*d 3FFE:8030::/28   3FFE:700:20:1::11 00:24:20 293 1275 559 8933 i
```

The following sample output from the **show bgp ipv6 neighbors** command shows the flap statistics for IPv6 address 3FFE:700:20:1::11:

```
Router# show bgp ipv6 unicast neighbors 3FFE:700:20:1::11 flap-statistics

BGP table version is 32084, local router ID is 192.168.7.225
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          From            Flaps Duration Reuse    Path
*d 2001:668::/35    3FFE:700:20:1:: 4923  2d12h    00:59:50 293 1849 3257
*d 3FFE::/24        3FFE:700:20:1:: 4799  2d12h    00:59:30 293 1849 5609 4554
*d 3FFE:8030::/28   3FFE:700:20:1:: 95    11:48:24 00:23:20 293 1275 559 8933
```

The following sample output from the **show bgp ipv6 neighbors** command shows the received routes for IPv6 address 2000:0:0:4::2:

```
Router# show bgp ipv6 unicast neighbors 2000:0:0:4::2 received-routes

BGP table version is 2443, local router ID is 192.168.0.2
Status codes:s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes:i - IGP, e - EGP, ? - incomplete

Network                Next Hop           Metric LocPrf Weight Path
*> 2000:0:0:1::/64      2000:0:0:4::2                        0 2 1 i
*> 2000:0:0:2::/64      2000:0:0:4::2                        0 2 i
*> 2000:0:0:2:1::/80    2000:0:0:4::2                        0 2 ?
*> 2000:0:0:3::/64      2000:0:0:4::2                        0 2 ?
*  2000:0:0:4::1/64     2000:0:0:4::2                        0 2 ?
```

Related Commands

Command	Description
neighbor activate	Enables the exchange of information with a neighboring router.

show bgp ipv6 paths

To display all the IPv6 Border Gateway Protocol (BGP) paths in the database, use the **show bgp ipv6 paths** command in user EXEC or privileged EXEC mode.

show bgp ipv6 {**unicast** | **multicast**} **paths** *regular-expression*

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.
regular-expression	Regular expression that is used to match the received paths in the database.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(2)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 Release 12.2(14)S.
12.3(2)T	The **unicast** keyword was added.
12.0(26)S	The **unicast** and **multicast** keywords were added.
12.3(4)T	The **multicast** keyword was 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.
12.2(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 bgp ipv6 unicast paths** and **show bgp ipv6 multicast paths** commands provide output similar to the **show ip bgp paths** command, except they are IPv6-specific.

The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the **unicast** keyword is mandatory starting with Cisco IOS Release 12.3(2)T.

The **multicast** keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

The following is sample output from the **show bgp ipv6 paths** command:

Note The output is the same whether or not the **unicast** or **multicast** keyword is used. The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and Cisco IOS Release 12.0(26)S and later, and the **multicast** keyword is available only in Cisco IOS Release 12.0(26)S and later releases.

```
Router# show bgp ipv6 unicast paths

Address    Hash Refcount Metric Path
0x61322A78    0        2      0 i
0x6131C214    3        2      0 6346 8664 786 i
0x6131D600   13        1      0 3748 1275 8319 1273 209 i
0x613229F0   17        1      0 3748 1275 8319 12853 i
0x61324AE0   18        1      1 4554 3748 4697 5408 i
0x61326818   32        1      1 4554 5609 i
0x61324728   34        1      0 6346 8664 9009 ?
0x61323804   35        1      0 3748 1275 8319 i
0x61327918   35        1      0 237 2839 8664 ?
0x61320504   38        2      0 3748 4697 1752 i
0x61320988   41        2      0 1849 786 i
0x6132245C   46        1      0 6346 8664 4927 i
```

Table 122 describes the significant fields shown in the display.

Table 122 show bgp ipv6 paths Field Descriptions

Field	Description
Address	Internal address where the path is stored.
Hash	Hash bucket where the path is stored.
Refcount	Number of routes using that path.
Metric	The Multi Exit Discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.)
Path	The autonomous system path for that route, followed by the origin code for that route.

show bgp ipv6 peer-group

To display information about Border Gateway Protocol (BGP) peer groups, use the **show bgp ipv6 peer-group** command in user EXEC or privileged EXEC mode.

show bgp ipv6 {**unicast** | **multicast**} **peer-group** [*name*]

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.
name	(Optional) Peer group name.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.0(26)S	The **unicast** and **multicast** keywords were added.
12.3(4)T	The **unicast** and **multicast** keywords were added.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.

Usage Guidelines

If a user does not specify a peer group name, then all BGP peer groups will be displayed.

The **multicast** keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

The following is sample output from the **show bgp ipv6 peer-group** command:

```
Router# show bgp ipv6 unicast peer-group

BGP peer-group is external-peerings,  remote AS 20
  BGP version 4
  Default minimum time between advertisement runs is 30 seconds

 For address family:IPv6 Unicast
  BGP neighbor is external-peerings, peer-group external, members:
  1::1
  Index 0, Offset 0, Mask 0x0
  Update messages formatted 0, replicated 0
  Number of NLRIs in the update sent:max 0, min 0
```

Table 123 describes the significant fields shown in the display.

Table 123 show bgp ipv6 peer-group Field Descriptions

Field	Description
BGP peer-group is	Type of BGP peer group.
remote AS	Autonomous system of the peer group.
BGP version	BGP version being used to communicate with the remote router.
For address family: IPv4 Unicast	IPv6 unicast-specific properties of this neighbor.

show bgp ipv6 prefix-list

To display routes that match a prefix list, use the **show bgp ipv6 prefix-list** command in user EXEC or privileged EXEC mode.

show bgp ipv6 {**unicast** | **multicast**} **prefix-list** *name*

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.
name	The specified prefix list.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.0(26)S	The **unicast** and **multicast** keywords were added.
12.3(4)T	The **unicast** and **multicast** keywords were added.

Usage Guidelines

The specified prefix list must be an IPv6 prefix list, which is similar in format to an IPv4 prefix list.

The **multicast** keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

The following is sample output from the **show bgp ipv6 prefix-list** command:

```
Router# show bgp ipv6 unicast prefix-list pin

ipv6 prefix-list pin:
   count:4, range entries:3, sequences:5 - 20, refcount:2
   seq 5 permit 747::/16 (hit count:1, refcount:2)
   seq 10 permit 747:1::/32 ge 64 le 64 (hit count:2, refcount:2)
   seq 15 permit 747::/32 ge 33 (hit count:1, refcount:1)
   seq 20 permit 777::/16 le 124 (hit count:2, refcount:1)

The ipv6 prefix-list match the following prefixes:

   seq 5: matches the exact match 747::/16
   seq 10:first 32 bits in prefix must match with a prefixlen of /64
   seq 15:first 32 bits in prefix must match with any prefixlen up to /128
   seq 20:first 16 bits in prefix must match with any prefixlen up to /124
```

Table 124 describes the significant fields shown in the display.

Table 124 show bgp ipv6 prefix-list Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	A 32-bit number written as 4 octets separated by periods (dotted-decimal format).
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s—The table entry is suppressed. • d—The table entry is dampened. • h—The table entry is history. • *—The table entry is valid. • >—The table entry is the best entry to use for that network. • i—The table entry was learned via an internal BGP session.
Origin codes	Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: • i—Entry originated from the Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • e—Entry originated from the Exterior Gateway Protocol (EGP). • ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IPv6 address of the network the entry describes.
Next Hop	IPv6 address of the next system that is used when forwarding a packet to the destination network. An entry of two colons (::) indicates that the router has some non-BGP routes to this network.
Metric	The value of the interautonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

show bgp ipv6 quote-regexp

To display IPv6 Border Gateway Protocol (BGP) routes matching the autonomous system path regular expression as a quoted string of characters, use the **show bgp ipv6 quote-regexp** command in user EXEC or privileged EXEC mode.

show bgp ipv6 {**unicast** | **multicast**} **quote-regexp** *regular-expression*

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.
regular-expression	Regular expression that is used to match the BGP autonomous system paths.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(2)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 Release 12.2(14)S.
12.3(2)T	The **unicast** keyword was added.
12.0(26)S	The **unicast** and **multicast** keywords were added.
12.3(4)T	The **multicast** keyword was 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.
12.2(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 bgp ipv6 unicast quote-regexp** and **show bgp ipv6 multicast quote-regexp** commands provide output similar to the **show ip bgp quote-regexp** command, except they are IPv6-specific.

The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the **unicast** keyword is mandatory starting with Cisco IOS Release 12.3(2)T.

The **multicast** keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

The following is sample output from the **show bgp ipv6 quote-regexp** command that shows paths beginning with 33 or containing 293:

Note The output is the same whether or not the **unicast** or **multicast** keyword is used. The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and Cisco IOS Release 12.0(26)S and later, and the **multicast** keyword is available only in Cisco IOS Release 12.0(26)S and later releases.

```
Router# show bgp ipv6 unicast quote-regexp ^33|293

BGP table version is 69964, local router ID is 192.31.7.225
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*  2001:200::/35    3FFE:C00:E:4::2          1             0 4554 293 3425 2500 i
*                   2001:0DB8:0:F004::1
                                                           0 3320 293 3425 2500 i
*  2001:208::/35    3FFE:C00:E:4::2          1             0 4554 293 7610 i
*  2001:228::/35    3FFE:C00:E:F::2                        0 6389 1849 293 2713 i
*  3FFE::/24        3FFE:C00:E:5::2                        0 33 1849 4554 i
*  3FFE:100::/24    3FFE:C00:E:5::2                        0 33 1849 3263 i
*  3FFE:300::/24    3FFE:C00:E:5::2                        0 33 293 1275 1717 i
*                   3FFE:C00:E:F::2                        0 6389 1849 293 1275
```

Note The caret (^) symbol in the example is a regular expression that is entered by pressing the Shift and 6 keys on your keyboard. A caret (^) symbol at the beginning of a regular expression matches the start of a line.

Table 125 describes the significant fields shown in the display.

Table 125 show bgp ipv6 quote-regexp Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	A 32-bit number written as 4 octets separated by periods (dotted-decimal format).
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s—The table entry is suppressed. • d—The table entry is dampened. • h—The table entry is history. • *—The table entry is valid. • >—The table entry is the best entry to use for that network. • i—The table entry was learned via an internal BGP session.

Table 125 show bgp ipv6 quote-regexp Field Descriptions (continued)

Field	Description
Origin codes	Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: • i—Entry originated from the Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • e—Entry originated from the Exterior Gateway Protocol (EGP). • ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IPv6 address of the network the entry describes.
Next Hop	IPv6 address of the next system that is used when forwarding a packet to the destination network. An entry of two colons (::) indicates that the router has some non-BGP routes to this network.
Metric	The value of the interautonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

Related Commands

Command	Description
show bgp ipv6 regexp	Displays IPv6 BGP routes matching the autonomous system path regular expression.
show ip bgp regexp	Displays routes matching the regular expression.

show bgp ipv6 regexp

To display IPv6 Border Gateway Protocol (BGP) routes matching the autonomous system path regular expression, use the **show bgp ipv6 regexp** command in user EXEC or privileged EXEC mode.

show bgp ipv6 {**unicast** | **multicast**} **regexp** *regular-expression*

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.
regular-expression	Regular expression that is used to match the BGP autonomous system paths.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(2)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 Release 12.2(14)S.
12.3(2)T	The **unicast** keyword was added.
12.0(26)S	The **unicast** and **multicast** keywords were added.
12.3(4)T	The **multicast** keyword was 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.
12.2(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 bgp ipv6 unicast regexp** and **show bgp ipv6 multicast regexp** commands provide output similar to the **show ip bgp regexp** command, except they are IPv6-specific.

The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the **unicast** keyword is mandatory starting with Cisco IOS Release 12.3(2)T.

The **multicast** keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

The following is sample output from the **show bgp ipv6 regexp** command that shows paths beginning with 33 or containing 293:

Note The output is the same whether or not the **unicast** or **multicast** keyword is used. The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and Cisco IOS Release 12.0(26)S and later, and the **multicast** keyword is available only in Cisco IOS Release 12.0(26)S and later releases.

```
Router# show bgp ipv6 unicast regexp ^33|293

BGP table version is 69964, local router ID is 192.168.7.225
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*  2001:200::/35    3FFE:C00:E:4::2          1             0 4554 293 3425 2500 i
*                   2001:0DB8:0:F004::1
                                                           0 3320 293 3425 2500 i
*  2001:208::/35    3FFE:C00:E:4::2          1             0 4554 293 7610 i
*  2001:228::/35    3FFE:C00:E:F::2                        0 6389 1849 293 2713 i
*  3FFE::/24        3FFE:C00:E:5::2                        0 33 1849 4554 i
*  3FFE:100::/24    3FFE:C00:E:5::2                        0 33 1849 3263 i
*  3FFE:300::/24    3FFE:C00:E:5::2                        0 33 293 1275 1717 i
*                   3FFE:C00:E:F::2                        0 6389 1849 293 1275
```

Note The caret (^) symbol in the example is a regular expression that is entered by pressing the Shift and 6 keys on your keyboard. A caret (^) symbol at the beginning of a regular expression matches the start of a line.

Table 126 describes the significant fields shown in the display.

Table 126 show bgp ipv6 regexp Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	A 32-bit number written as 4 octets separated by periods (dotted-decimal format).
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s—The table entry is suppressed. • d—The table entry is dampened. • h—The table entry is history. • *—The table entry is valid. • >—The table entry is the best entry to use for that network. • i—The table entry was learned via an internal BGP session.

Table 126 show bgp ipv6 regexp Field Descriptions (continued)

Field	Description
Origin codes	Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: • i—Entry originated from the Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • e—Entry originated from the Exterior Gateway Protocol (EGP). • ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IPv6 address of the network the entry describes.
Next Hop	IPv6 address of the next system that is used when forwarding a packet to the destination network. An entry of two colons (::) indicates that the router has some non-BGP routes to this network.
Metric	The value of the interautonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

show bgp ipv6 route-map

To display IPv6 Border Gateway Protocol (BGP) routes that failed to install in the routing table, use the **show bgp ipv6 route-map** command in user EXEC or privileged EXEC mode.

show bgp ipv6 {**unicast** | **multicast**} **route-map** *name*

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.
name	A specified route map to match.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.0(26)S	The **unicast** and **multicast** keywords were added.
12.3(4)T	The **unicast** and **multicast** keywords were added.

Usage Guidelines

The **multicast** keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

The following is sample output from the **show bgp ipv6 route-map** command for a route map named rmap:

```
Router# show bgp ipv6 unicast route-map rmap

BGP table version is 16, local router ID is 172.30.242.1
Status codes:s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes:i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*>i12:12::/64       2001:0DB8:101::1         0    100     50 ?
*>i12:13::/64       2001:0DB8:101::1         0    100     50 ?
*>i12:14::/64       2001:0DB8:101::1         0    100     50 ?
*>i543::/64         2001:0DB8:101::1         0    100     50 ?
```

Table 127 describes the significant fields shown in the display.

Table 127 show bgp ipv6 route-map Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	A 32-bit number written as 4 octets separated by periods (dotted-decimal format).
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s—The table entry is suppressed. • d—The table entry is dampened. • h—The table entry is history. • *—The table entry is valid. • >—The table entry is the best entry to use for that network. • i—The table entry was learned via an internal BGP session. • r —A RIB failure has occurred. • S—The route map is stale.
Origin codes	Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: • i—Entry originated from the Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • e—Entry originated from the Exterior Gateway Protocol (EGP). • ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IPv6 address of the network the entry describes.
Next Hop	IPv6 address of the next system that is used when forwarding a packet to the destination network. An entry of two colons (::) indicates that the router has some non-BGP routes to this network.
Metric	The value of the interautonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

show bgp ipv6 summary

To display the status of all IPv6 Border Gateway Protocol (BGP) connections, use the **show bgp ipv6 summary** command in user EXEC or privileged EXEC mode.

show bgp ipv6 {**unicast** | **multicast**} **summary**

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(2)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 Release 12.2(14)S.
12.3(2)T	The **unicast** keyword was added.
12.0(26)S	The **unicast** and **multicast** keywords were added.
12.3(4)T	The **unicast** and **multicast** keywords 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.
12.2(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 introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The **show bgp ipv6 unicast summary** and **show bgp ipv6 multicast summary** commands provide output similar to the **show ip bgp summary** command, except they are IPv6-specific.

The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the **unicast** keyword is mandatory starting with Cisco IOS Release 12.3(2)T.

The **multicast** keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

The following is sample output from the **show bgp ipv6 summary** command:

Note The output is the same whether or not the **unicast** or **multicast** keyword is used. The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and Cisco IOS Release 12.0(26)S and later, and the **multicast** keyword is available only in Cisco IOS Release 12.0(26)S and later releases.

```
Router# show bgp ipv6 unicast summary

BGP router identifier 172.30.4.4, local AS number 200
BGP table version is 1, main routing table version 1

Neighbor           V    AS  MsgRcvd  MsgSent   TblVer  InQ  OutQ  Up/Down   State/PfxRcd
2001:0DB8:101::2   4    200    6869     6882        0    0     0  06:25:24  Active
```

Table 128 describes the significant fields shown in the display.

Table 128 show bgp ipv6 summary Field Descriptions

Field	Description
BGP router identifier	IP address of the networking device.
BGP table version	Internal version number of the BGP database.
main routing table version	Last version of BGP database that was injected into the main routing table.
Neighbor	IPv6 address of a neighbor.
V	BGP version number spoken to that neighbor.
AS	Autonomous system.
MsgRcvd	BGP messages received from that neighbor.
MsgSent	BGP messages sent to that neighbor.
TblVer	Last version of the BGP database that was sent to that neighbor.
InQ	Number of messages from that neighbor waiting to be processed.
OutQ	Number of messages waiting to be sent to that neighbor.
Up/Down	The length of time that the BGP session has been in state Established, or the current state if it is not Established.
State/PfxRcd	Current state of the BGP session/the number of prefixes the router has received from a neighbor or peer group. When the maximum number (as set by the **neighbor maximum-prefix** command) is reached, the string "PfxRcd" appears in the entry, the neighbor is shut down, and the connection is Idle. An (Admin) entry with Idle status indicates that the connection has been shut down using the **neighbor shutdown** command.

Related Commands

Command	Description
clear bgp ipv6	Resets an IPv6 BGP TCP connection using BGP soft reconfiguration.
neighbor maximum-prefix	Controls how many prefixes can be received from a neighbor.
neighbor shutdown	Disables a neighbor or peer group.

show bgp vpnv6 unicast

To display Virtual Private Network (VPN) entries in a Border Gateway Protocol (BGP) table, use the **show bgp vpnv6 unicast** command in user EXEC or privileged EXEC mode.

show bgp vpnv6 unicast [**all** | **vrf** [*vrf-name*]]

Syntax Description

all	(Optional) Displays all entries in a BGP table.
vrf	(Optional) Specifies all VPN routing and forwarding (VRF) instance tables or a specific VRF table for IPv4 or IPv6 address.
vrf-name	(Optional) Names a specific VRF table for an IPv4 or IPv6 address.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
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.

Usage Guidelines

BGP is used for distributing VPN IPv6 routing information in the VPN backbone. The local routes placed in the BGP routing table on an egress provider edge (PE) router are distributed to other PE routers.

Examples

The following examples shows BGP entries from all of the customer-specific IPv6 routing tables:

```
Router# show bgp vpnv6 unicast all

Network                   Next Hop              Metric LocPrf    Weight Path
Route Distinguisher: 100:1
*  2001:100:1:1000::/56   2001:100:1:1000::72a    0               0     200 ?
*                         ::                 0                     32768 ?
*  i2001:100:1:2000::/56  ::FFFF:200.10.10.1
Route Distinguisher: 200:1
*  2001:100:2:1000::/56   ::               0                      32768 ?
*  2001:100:2:2000::/56   ::FFFF:200.10.10.1      0                32768 ?
```

Table 129 describes the significant fields shown in the displays.

Table 129 show bgp vpnv6 unicast Field Descriptions

Field	Description
Network	IPv6 address of the network the entry describes.
Next Hop	IPv6 address of the next system that is used when forwarding a packet to the destination network. An entry of two colons (::) indicates that the router has some non-BGP routes to this network.
Metric	If shown, this is the value of the interautonomous system metric. This field is frequently not used.
Loc Prf	Local preference value as configured with the **set local-preference** command.
Weight	Weight of the route as set through autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path. At the end of the path is the origin code for the path. It can be one of the following values: • i—The entry was originated with the IGP and advertised with a network router configuration command. • e—The route originated with EGP. • ?—The origin of the path is not clear. Usually this is a path that is redistributed into BGP from an IGP.
Route Distinguisher:	Specifies the VRF instance.

show call active fax

To display call information for T.37 store-and-forward fax transmissions in progress, use the **show call active fax** command in user EXEC or privileged EXEC mode.

show call active fax [**brief** [**id** *identifier*] | **compact** [**duration** {**less** *seconds* | **more** *seconds*}] | **id** *identifier*]

Syntax Description

brief	(Optional) Displays a truncated version of fax call information.
id *identifier*	(Optional) Displays only the call with the specified *identifier*. Range is a hex value from 1 to FFFF.
compact	(Optional) Displays a compact version of the fax call information.
duration	(Optional) Displays active calls that are longer or shorter than a specified *seconds* value. The arguments and keywords are as follows: • **less**—Displays calls shorter than the *seconds* value. • **more**—Displays calls longer than the *seconds* value. • *seconds*—Elapsed time, in seconds. Range is from 1 to 2147483647. There is no default value.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 2600 series and Cisco 3600 series.
12.0(3)XG	This command was modified. Support for Voice over Frame Relay (VoFR) was added.
12.0(4)XJ	This command was implemented for store-and-forward fax on the Cisco AS5300.
12.0(4)T	This command was implemented on the Cisco 7200 series.
12.0(7)XK	This command was implemented on the Cisco MC3810.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(3)T	This command was modified. This command was implemented for modem pass-through over VoIP on the Cisco AS5300.
12.1(5)XM	This command was implemented on the Cisco AS5800.
12.1(5)XM2	The command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support was not included for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850.
12.2(11)T	Support was added for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850.

Release	Modification
12.3(14)T	This command was modified. 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.
12.4(2)T	This command was modified. The LocalHostname display field was added to the VoIP call leg record.
12.4(15)T	This command was modified. The Port and BearerChannel display fields were added to the TELE call leg record of the command output.
12.4(16)	This command was modified. The Port and BearerChannel display fields were added to the TELE call leg record of the command output.
12.4(22)T	This command was modified. Command output was updated to show IPv6 information.

Usage Guidelines

Use this command to display the contents of the active call table. This command displays information about call times, dial peers, connections, quality of service, and other status and statistical information for T.37 store-and-forward fax calls currently connected through the router. This command works with both on-ramp and off-ramp store-and-forward fax functions.

To display information about fax relay calls in progress, use the **show call active voice** command.

Examples

The following is sample output from the **show call active fax** command:

```
Router# show call active fax

GENERIC:
SetupTime=22021 ms
Index=1
PeerAddress=peer one
PeerSubAddress=
PeerId=0
PeerIfIndex=0
LogicalIfIndex=0
ConnectTime=24284
CallState=4
CallOrigin=2
ChargedUnits=0
InfoType=10
TransmitPackets=0
TransmitBytes=0
ReceivePackets=0
ReceiveBytes=41190

MMOIP:
ConnectionId[0x37EC7F41 0xB0110001 0x0 0x35C34]
CallID=1
RemoteIPAddress=10.0.0.0
SessionProtocol=SMTP
SessionTarget=
MessageId=
AccountId=
ImgEncodingType=MH
ImgResolution=fine
AcceptedMimeTypes=2
DiscardedMimeTypes=1
Notification=None
```

```
GENERIC:
SetupTime=23193 ms
Index=1
PeerAddress=527....
PeerSubAddress=
PeerId=3469
PeerIfIndex=157
LogicalIfIndex=30
ConnectTime=24284
CallState=4
CallOrigin=1
ChargedUnits=0
InfoType=10
TransmitPackets=5
TransmitBytes=6513
ReceivePackets=0
ReceiveBytes=0

TELE:
ConnectionId=[0x37EC7F41 0xB0110001 0x0 0x35C34]
CallID=2
Port=3/0/0 (2)
BearerChannel=3/0/0.1
TxDuration=24010 ms
FaxTxDuration=10910 ms
FaxRate=14400
NoiseLevel=-1
ACOMLevel=-1
OutSignalLevel=0
InSignalLevel=0
InfoActivity=0
ERLLevel=-1
SessionTarget=
ImgPages=0
```

Table 130 provides an alphabetical listing of the fields displayed in the output of the **show call active fax** command and a description of each field.

Table 130 show call active fax Field Descriptions

Field	Description
ACOM Level	Current ACOM level for this call. ACOM is the combined loss achieved by the echo canceler, which is the sum of the Echo Return Loss, Echo Return Loss Enhancement, and nonlinear processing loss for the call.
BearerChannel	Identification of the bearer channel carrying the call.
Buffer Drain Events	Total number of jitter buffer drain events.
Buffer Fill Events	Total number of jitter buffer fill events.
CallDuration	Length of the call, in hours, minutes, and seconds, hh:mm:ss.
CallOrigin	Call origin: answer or originate.
CallState	Current state of the call.
ChargedUnits	Total number of charging units that apply to this peer since system startup. The unit of measure for this field is hundredths of second.
CodecBytes	Payload size, in bytes, for the codec used.

Table 130 show call active fax Field Descriptions (continued)

Field	Description
CoderTypeRate	Negotiated coder rate. This value specifies the send rate of voice or fax compression to its associated call leg for this call.
ConnectionId	Global call identifier for this gateway call.
ConnectTime	Time, in milliseconds, at which the call was connected.
Consecutive-packets-lost Events	Total number of consecutive (two or more) packet-loss events.
Corrected packet-loss Events	Total number of packet-loss events that were corrected using the RFC 2198 method.
Dial-Peer	Tag of the dial peer sending this call.
EchoCancellerMaxReflector=64	The location of the largest reflector, in milliseconds (ms). The reflector size does not exceed the configured echo path capacity. For example, if 32 ms is configured, the reflector does not report beyond 32 ms.
ERLLevel	Current echo return loss (ERL) level for this call.
FaxTxDuration	Duration of fax transmission from this peer to the voice gateway for this call. You can derive the Fax Utilization Rate by dividing the FaxTxDuration value by the TxDuration value.
GapFillWithInterpolation	Duration of a voice signal played out with a signal synthesized from parameters, or samples of data preceding and following in time because voice data was lost or not received in time from the voice gateway for this call.
GapFillWithPrediction	Duration of the voice signal played out with signal synthesized from parameters, or samples of data preceding in time, because voice data was lost or not received in time from the voice gateway for this call. Examples of such pullout are frame-eraser and frame-concealment strategies in G.729 and G.723.1 compression algorithms.
GapFillWithRedundancy	Duration of a voice signal played out with a signal synthesized from available redundancy parameters because voice data was lost or not received in time from the voice gateway for this call.
GapFillWithSilence	Duration of a voice signal replaced with silence because voice data was lost or not received in time for this call.
GENERIC	Generic or common parameters, that is, parameters that are common for VoIP and telephony call legs.
H323 call-legs	Total H.323 call legs for which call records are available.
HiWaterPlayoutDelay	High-water-mark Voice Playout FIFO Delay during this call, in ms.
Index	Dial peer identification number.
InfoActivity	Active information transfer activity state for this call.
InfoType	Information type for this call; for example, voice or fax.
InSignalLevel	Active input signal level from the telephony interface used by this call.
Last Buffer Drain/Fill Event	Elapsed time since the last jitter buffer drain or fill event, in seconds.
LocalHostname	Local hostnames used for locally generated gateway URLs.

Table 130 show call active fax Field Descriptions (continued)

Field	Description
LogicalIfIndex	Index number of the logical interface for this call.
LoWaterPlayoutDelay	Low-water-mark Voice Playout FIFO Delay during this call, in ms.
LowerIFName	Physical lower interface information. Appears only if the medium is ATM, Frame Relay (FR), or High-Level Data Link Control (HDLC).
Media	Medium over which the call is carried. If the call is carried over the (telephone) access side, the entry is TELE. If the call is carried over the voice network side, the entry is either ATM, FR, or HDLC.
Modem passthrough signaling method in use	Indicates that this is a modem pass-through call and that named signaling events (NSEs)—a Cisco-proprietary version of named telephone events in RFC 2833—are used for signaling codec upspeed. The upspeed method is the method used to dynamically change the codec type and speed to meet network conditions. This means that you might move to a faster codec when you have both voice and data calls and then slow down when there is only voice traffic.
NoiseLevel	Active noise level for this call.
OnTimeRvPlayout	Duration of voice playout from data received on time for this call. Derive the Total Voice Playout Duration for Active Voice by adding the OnTimeRvPlayout value to the GapFill values.
OutSignalLevel	Active output signal level to the telephony interface used by this call.
PeerAddress	Destination pattern or number associated with this peer.
PeerId	ID value of the peer table entry to which this call was made.
PeerIfIndex	Voice port index number for this peer. For ISDN media, this would be the index number of the B channel used for this call.
PeerSubAddress	Subaddress when this call is connected.
Percent Packet Loss	Total percent packet loss.
Port	Identification of the time-division multiplexing (TDM) voice port carrying the call.
ReceiveBytes	Number of bytes received by the peer during this call.
ReceiveDelay	Average Playout FIFO Delay plus the Decoder Delay during this voice call, in ms.
ReceivePackets	Number of packets received by this peer during this call.
ReleaseSource	Number value of the release source.
RemoteIPAddress	Remote system IP address for the VoIP call.
RemoteUDPPort	Remote system User Datagram Protocol (UDP) listener port to which voice packets are sent.
RoundTripDelay	Voice packet round-trip delay between the local and remote systems on the IP backbone for this call.
SelectedQoS	Selected Resourse Reservation Protocol (RSVP) quality of service (QoS) for this call.

Table 130 show call active fax Field Descriptions (continued)

Field	Description
SessionProtocol	Session protocol used for an Internet call between the local and remote routers through the IP backbone.
SessionTarget	Session target of the peer used for this call.
SetupTime	Value of the system UpTime, in milliseconds, when the call associated with this entry was started.
SignalingType	Signaling type for this call; for example, channel-associated signaling (CAS) or common channel signaling (CCS).
SIP call-legs	Total Session Initiation Protocol (SIP) call legs for which call records are available.
Telephony call-legs	Total telephony call legs for which call records are available.
Time between Buffer Drain/Fills	Minimum and maximum durations between jitter buffer drain or fill events, in seconds.
TransmitBytes	Number of bytes sent by this peer during this call.
TransmitPackets	Number of packets sent by this peer during this call.
TxDuration	The length of the call. Appears only if the medium is TELE.
VAD	Whether voice activation detection (VAD) was enabled for this call.
VoiceTxDuration	Duration of voice transmission from this peer to the voice gateway for this call, in ms. Derive the Voice Utilization Rate by dividing the VoiceTxDuration value by the TxDuration value.

The following is sample output from the **show call active fax brief** command:

```
Router# show call active fax brief

<ID>: <start>hs.<index> +<connect> pid:<peer_id> <dir> <addr> <state> \
  tx:<packets>/<bytes> rx:<packets>/<bytes> <state>
IP <ip>:<udp> rtt:<time>ms pl:<play>/<gap>ms lost:<lost>/<early>/<late>
  delay:<last>/<min>/<max>ms <codec>
FR <protocol> [int dlci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
  sig:<on/off> <codec> (payload size)
Tele <int>: tx:<tot>/<v>/<fax>ms <codec> noise:<l> acom:<l> i/o:<l>/<l> dBm

1    : 22021hs.1 +2263 pid:0 Answer wook song active
tx:0/0 rx:0/41190
IP 0.0.0.0 AcceptedMime:2 DiscardedMime:1

1    : 23193hs.1 +1091 pid:3469 Originate 527.... active
tx:10/13838 rx:0/0
Tele : tx:31200/10910/20290ms  noise:-1 acom:-1  i/0:0/0 dBm
```

The following is sample output from the **show call active fax** command displaying T.38 fax relay statistics:

```
Router# show call active fax

Telephony call-legs: 1
SIP call-legs: 0
H323 call-legs: 0
MGCP call-legs: 0
Multicast call-legs: 0
```

```
Total call-legs: 1

 GENERIC:
SetupTime=1874690 ms
Index=1
PeerAddress=5551234
PeerSubAddress=
PeerId=3
PeerIfIndex=244
LogicalIfIndex=118
ConnectTime=187875
CallDuration=00:00:44 sec
CallState=4
CallOrigin=2
ChargedUnits=0
InfoType=fax
TransmitPackets=309
TransmitBytes=5661
ReceivePackets=1124
ReceiveBytes=49189
TELE:
ConnectionId=[0x6B241E98 0xA78111D8 0x8002000A 0xF4107CA0]
IncomingConnectionId=[0x6B241E98 0xA78111D8 0x8002000A 0xF4107CA0]
CallID=1
Port=3/0/0 (1)
BearerChannel=3/0/0.1
TxDuration=2840 ms
VoiceTxDuration=0 ms
FaxTxDuration=0 ms
FaxRate=disable bps
FaxRelayMaxJitBufDepth 346
FaxRelayJitterBufOverflow 0
Initial HS Modulation is V.17/long/14400
Recent HS modulation is V.17/short/14400
Number of pages 1
Direction of transmission is Transmit
Num of Packets TX'ed/RX'ed 932/52
Packet loss conceal is 0
Encapsulation protocol is T.38 (UDPTL)
ECM is DISABLED
NoiseLevel=0
ACOMLevel=0
OutSignalLevel=0
InSignalLevel=0
InfoActivity=0
ERLLevel=0
SessionTarget=
ImgPages=0
CallerName=
CallerIDBlocked=False
OriginalCallingNumber=5551234
OriginalCallingOctet=0x80
OriginalCalledNumber=5555678
OriginalCalledOctet=0x80
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0xFF
TranslatedCallingNumber=5551234
TranslatedCallingOctet=0x80
TranslatedCalledNumber=5555678
TranslatedCalledOctet=0x80
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0xFF
GwReceivedCalledNumber=5555678
GwReceivedCalledOctet3=0x80
```

```
GwReceivedCallingNumber=5551234
GwReceivedCallingOctet3=0x80
GwReceivedCallingOctet3a=0x0
DSPIdentifier=1/0:0
Telephony call-legs: 1
SIP call-legs: 0
H323 call-legs: 0
MGCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 1
```

Table 131 provides an alphabetical listing of the fields displayed in the output of the **show call active fax** command for T.38 fax relay statistics and a description of each field.

Table 131 show call active fax Field Descriptions for Significant T.38 Fax Relay Statistics

Field	Description
ACOMLevel	Current ACOM level estimate in 0.1 dB increments. The term ACOM is used in G.165, *General Characteristics of International Telephone Connections and International Telephone Circuits: Echo Cancellers*. ACOM is the combined loss achieved by the echo canceller, which is the sum of the ERL, ERL enhancement, and nonlinear processing loss for the call.
BearerChannel	Identification of the bearer channel carrying the call.
ERLLevel	Current ERL level estimate in 0.1 dB increments.
FaxRate	Fax transmission rate from this peer to the specified dial peer, in bits per second (bps).
FaxRelayJitterBufOverflow	Fax relay jitter buffer overflow, in ms.
FaxRelayMaxJitBufDepth	Fax relay maximum jitter buffer depth, in ms.
FaxTxDuration	Duration of fax transmission from this peer to the voice gateway for this call, in ms.
GwReceivedCalledNumber, GwReceivedCalledOctet3	Call information received at the gateway.
H323 call-legs	Type of call: H.323.
Initial HS Modulation	Initial high speed modulation used.
LogicalIfIndex	Index number of the logical interface for this call.
MGCP call-legs	Type of call: Media Gateway Control Protocol (MGCP).
Multicast call-legs	Type of call: Multicast.
OriginalCallingNumber, OriginalCalling Octet, OriginalCalledNumber, OriginalCalledOctet, OriginalRedirectCalledNumber, OriginalRedirectCalledOctet	Original call information regarding calling, called, and redirect numbers, and octet-3s. Octet-3s are information elements (IEs) of Q.931 that include type of number, numbering plan indicator, presentation indicator, and redirect reason information.
PeerIfIndex	Voice port index number for this peer. For ISDN media, this would be the index number of the B channel used for this call.
Port	Identification of the TDM voice port carrying the call.
Recent HS Modulation	Most recent high-speed modulation used.

Table 131 show call active fax Field Descriptions for Significant T.38 Fax Relay Statistics

Field	Description
SIP call-legs	Type of call: SIP.
Telephony call-legs	Type of call: Telephony.
Total call-legs	Total calls.
TranslatedCallingNumber, TranslatedCallingOctet, TranslatedCalledNumber, TranslatedCalledOctet, TranslatedRedirectCalledNumber, TranslatedRedirectCalledOctet	Translated call information.
TxDuration	Duration of transmit path open from this peer to the voice gateway for this call, in ms.
VoiceTxDuration	Duration of voice transmission from this peer to the voice gateway for this call, in ms.

Related Commands

Command	Description
show call active voice	Displays call information for voice calls that are in progress.
show call history	Displays the call history table.
show call-router routes	Displays the dynamic routes in the cache of the BE.
show call-router status	Displays the Annex G BE status.
show voice port	Displays configuration information about a specific voice port.

show call active voice

To display call information for voice calls in progress, use the **show call active voice** command in user EXEC or privileged EXEC mode.

show call active voice [[**brief**] [**long-dur-call-inactive** | **media-inactive**] [**called-number** *number* | **calling-number** *number*] [**id** *call-identifier*] | **compact** [**duration** {**less** | **more**} *seconds*] | **echo-canceller** {*hexadecimal-id* | **port** *slot-number* | **summary**} | **long-dur-call** [**called-number** *number* | **calling-number** *number*] | **redirect tbct** | **stats**]

Syntax in Cisco IOS Release 12.2(33)SXH and Subsequent 12.2SX Releases

show call active [**brief**]

Syntax Description

brief	(Optional) Displays a truncated version of call information.
long-dur-call-inactive	(Optional) Displays long duration calls that are detected and notified.
media-inactive	(Optional) Displays information about inactive media that have been detected.
called-number *number*	(Optional) Displays a specific called number pattern.
calling-number *number*	(Optional) Displays a specific calling number pattern.
id *call-identifier*	(Optional) Displays only the call with the specified *call-identifier* value. The range is from 1 to FFFF.
compact	(Optional) Displays a compact version of call information.
duration	(Optional) Displays the call history for the specified time duration.
less *seconds*	Displays the call history for shorter duration calls, in seconds. The range is from 1 to 2147483647.
more *seconds*	Displays the call history for longer duration calls, in seconds. The range is from 1 to 2147483647.
echo-canceller	(Optional) Displays information about the state of the extended echo canceller (EC).
hexadecimal-id	The hexadecimal ID of an active voice call. The range is from 0x0 to 0xFFFFFFFF.
port *slot-number*	Displays EC details for a specified active voice port. The range varies depending on the voice ports available on the router.
summary	Displays an EC summary for all active voice calls.
long-dur-call	(Optional) Displays long duration calls that are detected and notified.
redirect	(Optional) Displays information about active calls that are being redirected using Release-to-Pivot (RTPvt) or Two B-Channel Transfer (TBCT).
tbct	Displays information about TBCT calls.
stats	(Optional) Displays information about digital signal processing (DSP) voice quality metrics.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
11.3(1)T	This command was introduced.
12.0(3)XG	This command was modified. Support for Voice over Frame Relay (VoFR) was added.
12.0(4)XJ	This command was implemented for store-and-forward fax on the Cisco AS5300.
12.0(4)T	This command was implemented on the Cisco 7200 series.
12.0(7)XK	This command was implemented on the Cisco MC3810.
12.1(3)T	This command was implemented for modem pass-through over VoIP on the Cisco AS5300.
12.1(5)XM	This command was implemented on the Cisco AS5800.
12.1(5)XM2	The command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support was not included for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850.
12.2(11)T	Support was added for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850.
12.2(13)T	This command was modified. The **echo-canceller** keyword was added. The command output was modified with an extra reflector location when the extended EC is present; the largest reflector location is shown.
12.3(1)	This command was modified. The **redirect** keyword was added.
12.3(4)T	This command was modified. The **called-number**, **calling-number**, and **media-inactive** keywords were added.
12.3(14)T	This command was modified. New output relating to Skinny Client Control Protocol (SCCP), SCCP Telephony Control Application (STCAPP), and modem pass-through traffic was added.
12.4(2)T	This command was modified. The LocalHostname display field was added to the VoIP call leg record and command output was enhanced to display modem relay physical layer and error correction protocols.
12.4(4)T	This command was modified. The **long-dur-call** keyword was added.
12.4(11)XW	This command was modified. The **stats** keyword was added.
12.4(15)T	This command was modified. The Port and BearerChannel display fields were added to the TELE call leg record of the command output.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(16)	This command was modified. The Port and BearerChannel display fields were added to the TELE call leg record of the command output.
12.4(22)T	This command was modified. Command output was updated to show IPv6 information.

Usage Guidelines

Use this command to display the contents of the active voice call table. This command displays information about call times, dial peers, connections, and quality of service, and other status and statistical information for voice calls currently connected through the router.

Before you can query the echo state, you need to know the hexadecimal ID. To find the hexadecimal ID, enter the **show call active voice brief** command or use the **show voice call status** command.

When the extended EC is present, the **show call active voice** command displays the contents of the Ditech EC_CHAN_CTRL structure. Table 132 contains names and descriptions of the fields in the EC_CHAN_CTRL structure. Table 132 also provides a listing of the information types associated with this command.

Table 132 EC_CHAN_CTRL Field Descriptions

Symbol	Field	Description
BYP0	Channel bypass	• 1 = Transparent bypass; EC is disabled. • 0 = Cancel; EC is enabled.
TAIL3	Max tail	• 0 = 24 milliseconds. • 1 = 32 milliseconds. • 2 = 48 milliseconds. • 3 = 64 milliseconds. **Note** This field should be set just greater than the anticipated worst round-trip tail delay.
REC3	Residual echo control	• 0 = Cancel only; echo is the result of linear processing; no nonlinear processing is applied. • 1 = Suppress residual; residual echo is zeroed; simple nonlinear processing is applied (you might experience “dead air” when talking). • 2 = Reserved. • 3 = Generate comfort noise (default).
FRZ0	h-register hold	1 = Freezes h-register; used for testing.
HZ0	h-register clear	Sending the channel command with this bit set clears the h-register.
TD3	Modem tone disable	• 0 = Ignore 2100 Hz modem answer tone. • 1 = G.164 mode (bypass canceller if 2100 Hz tone). • 2 = R. • 3 = G.165 mode (bypass canceller for phase reversing tone only).
ERL0	Echo return loss	• 0 = 6 decibel (dB). • 1 = 3 dB. • 2 = 0 dB. • 3 = R. Worst echo return loss (ERL) situation in which canceller still works.
HLC1	High level compensation	• 0 = No attenuation. • 1 = 6 dB if clipped. On loud circuits, the received direction can be attenuated 6 dB if clipping is observed.
R0	Reserved	Must be set to 0 to ensure compatibility with future releases.

Use the **show call active voice redirect tbct** command to monitor any active calls that implement RTPvt or TBCT.

When a call is no longer active, its record is stored. You can display the record by using the **show call history voice** command.

Examples

The following is sample output from the **show call active voice** command for modem relay traffic:

```
Router# show call active voice

Modem Relay Local Rx Speed=0 bps
Modem Relay Local Tx Speed=0 bps
Modem Relay Remote Rx Speed=0 bps
Modem Relay Remote Tx Speed=0 bps
Modem Relay Phy Layer Protocol=v34
Modem Relay Ec Layer Protocol=v14
SPRTInfoFramesReceived=0
SPRTInfoTFramesSent=0
SPRTInfoTFramesResent=0
SPRTXidFramesReceived=0
SPRTXidFramesSent=0
SPRTTotalInfoBytesReceived=0
SPRTTotalInfoBytesSent=0
SPRTPacketDrops=0
```

Table 133 describes the significant fields shown in the display.

Table 133 show show call active voice Field Descriptions

Field	Description
Modem Relay Local Rx Speed	Download speed, in bits per second, of the local modem relay.
Modem Relay Local Tx Speed	Upload speed of the local modem relay.
Modem Relay Remote Rx Speed	Download speed of the remote modem relay.
Modem Relay Remote Tx Speed	Upload speed of the remote modem relay.
Modem Relay Phy Layer Protocol	Physical protocol of the modem relay.
Modem Relay Ec Layer Protocol	EC layer protocol of the modem relay.
SPRTInfoFramesReceived	Total number of simple packet relay transport (SPRT) protocol frames received.
SPRTInfoTFramesSent	Total number of SPRT frames sent.
SPRTInfoTFramesResent	Total number of SPRT frames sent again.
SPRTXidFramesReceived	Total number of SPRTS ID frames received.
SPRTXidFramesSent	Total number of SPRTS ID frames sent.
SPRTTotalInfoBytesReceived	Total number of SPRT bytes received.
SPRTTotalInfoBytesSent	Total number of SPRT bytes sent.
SPRTPacketDrops	Total number of SPRT packets dropped.

The following is sample output from the **show call active voice** command:

```
Router# show call active voice

Telephony call-legs: 1
SIP call-legs: 0
H323 call-legs: 1
```

```
Call agent controlled call-legs: 0
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 2

 GENERIC:
SetupTime=1072620 ms
Index=1
PeerAddress=9193927582
PeerSubAddress=
PeerId=8
PeerIfIndex=19
LogicalIfIndex=0
ConnectTime=1078940 ms
CallDuration=00:00:51 sec
CallState=4
CallOrigin=2
ChargedUnits=0
InfoType=speech
TransmitPackets=1490
TransmitBytes=0
ReceivePackets=2839
ReceiveBytes=56780
VOIP:
ConnectionId[0xE28B6D1D 0x3D9011D6 0x800400D0 0xBA0D97A1]
IncomingConnectionId[0xE28B6D1D 0x3D9011D6 0x800400D0 0xBA0D97A1]
CallID=1
RemoteIPAddress=10.44.44.44
RemoteUDPPort=17096
RemoteSignallingIPAddress=10.44.44.44
RemoteSignallingPort=56434
RemoteMediaIPAddress=10.44.44.44
RemoteMediaPort=17096
RoundTripDelay=6 ms
SelectedQoS=best-effort
tx_DtmfRelay=h245-signal
FastConnect=TRUE

AnnexE=FALSE

Separate H245 Connection=FALSE

H245 Tunneling=TRUE

SessionProtocol=cisco
ProtocolCallId=
SessionTarget=
OnTimeRvPlayout=54160
GapFillWithSilence=0 ms
GapFillWithPrediction=0 ms
GapFillWithInterpolation=0 ms
GapFillWithRedundancy=0 ms
HiWaterPlayoutDelay=70 ms
LoWaterPlayoutDelay=60 ms
TxPakNumber=1490
TxSignalPak=0
TxComfortNoisePak=1
TxDuration=54240
TxVoiceDuration=29790
RxPakNumber=2711
RxSignalPak=0
RxDuration=0
TxVoiceDuration=54210
VoiceRxDuration=54160
```

```
RxOutOfSeq=0
RxLatePak=0
RxEarlyPak=0
PlayDelayCurrent=60
PlayDelayMin=60
PlayDelayMax=70
PlayDelayClockOffset=212491899
PlayDelayJitter=0 ms
PlayErrPredictive=0
PlayErrInterpolative=0
PlayErrSilence=0
PlayErrBufferOverFlow=10
PlayErrRetroactive=0
PlayErrTalkspurt=0
OutSignalLevel=-57
InSignalLevel=-51
LevelTxPowerMean=0
LevelRxPowerMean=-510
LevelBgNoise=0
ERLLevel=16
ACOMLevel=16
ErrRxDrop=0
ErrTxDrop=0
ErrTxControl=0
ErrRxControl=0
ReceiveDelay=60 ms
LostPackets=0
EarlyPackets=0
LatePackets=0
SRTP = off
VAD = enabled
CoderTypeRate=g729r8
CodecBytes=20
Media Setting=flow-through
CallerName=
CallerIDBlocked=False
OriginalCallingNumber=9193927582
OriginalCallingOctet=0x21
OriginalCalledNumber=93615494
OriginalCalledOctet=0xC1
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0xFF
TranslatedCallingNumber=9193927582
TranslatedCallingOctet=0x21
TranslatedCalledNumber=93615494
TranslatedCalledOctet=0xC1
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0xFF
GwReceivedCalledNumber=93615494
GwReceivedCalledOctet3=0xC1
GwReceivedCallingNumber=9193927582
GwReceivedCallingOctet3=0x21
GwReceivedCallingOctet3a=0x81
MediaInactiveDetected=no
MediaInactiveTimestamp=
MediaControlReceived=
Username=

 GENERIC:
SetupTime=1072760 ms
Index=1
PeerAddress=93615494
PeerSubAddress=
PeerId=9
```

```
PeerIfIndex=18
LogicalIfIndex=4
ConnectTime=1078940 ms
CallDuration=00:00:53 sec
CallState=4
CallOrigin=1
ChargedUnits=0
InfoType=speech
TransmitPackets=2953
TransmitBytes=82684
ReceivePackets=1490
ReceiveBytes=29781
TELE:
ConnectionId=[0xE28B6D1D 0x3D9011D6 0x800400D0 0xBA0D97A1]
IncomingConnectionId=[0xE28B6D1D 0x3D9011D6 0x800400D0 0xBA0D97A1]
CallID=2
Port=3/0/0 (1)
BearerChannel=3/0/0.2
TxDuration=59080 ms
VoiceTxDuration=29790 ms
FaxTxDuration=0 ms
CoderTypeRate=g729r8
NoiseLevel=-54
ACOMLevel=16
OutSignalLevel=-57
InSignalLevel=-51
InfoActivity=1
ERLLevel=16
EchoCancellerMaxReflector=8
SessionTarget=
ImgPages=0
CallerName=
CallerIDBlocked=False
AlertTimepoint=1073340 ms
OriginalCallingNumber=9193927582
OriginalCallingOctet=0x21
OriginalCalledNumber=93615494
OriginalCalledOctet=0xC1
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0xFF
TranslatedCallingNumber=9193927582
TranslatedCallingOctet=0x21
TranslatedCalledNumber=93615494
TranslatedCalledOctet=0xC1
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0xFF
GwReceivedCalledNumber=93615494
GwReceivedCalledOctet3=0xC1
GwOutpulsedCalledNumber=93615494
GwOutpulsedCalledOctet3=0xC1
GwReceivedCallingNumber=9193927582
GwReceivedCallingOctet3=0x21
GwReceivedCallingOctet3a=0x81
GwOutpulsedCallingNumber=9193927582
GwOutpulsedCallingOctet3=0x21
GwOutpulsedCallingOctet3a=0x81
DSPIdentifier=3/1:1
Telephony call-legs: 1
SIP call-legs: 0
H323 call-legs: 1
Call agent controlled call-legs: 0
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 2
```

Table 132 on page 1727 and Table 134 describe the significant fields shown in the display, in alphabetical order.

Table 134 show call active voice Field Descriptions

Field	Description
CallDuration	Length of the call, in hours, minutes, and seconds, hh:mm:ss.
CallState	Current state of the call.
Call agent controlled call-legs	Displays call legs for devices that are not telephony endpoints; for example, transcoding and conferencing
ChargedUnits	Total number of charging units that apply to this peer since system startup. The unit of measure for this field is hundredths of second.
CodecBytes	Payload size, in bytes, for the codec used.
CoderTypeRate	Negotiated coder rate. This value specifies the send rate of voice or fax compression to its associated call leg for this call.
ConnectionId	Global call identifier for this gateway call.
ConnectTime	Time, in ms, during which the call was connected.
EchoCancellerMaxReflector	Size of the largest reflector, in ms. The reflector size cannot exceed the configured echo path capacity. For example, if 32 ms is configured, the reflector does not report capacity beyond 32 ms.
ERLLevel	Current echo return loss (ERL) level for this call.
FaxTxDuration	Duration, in ms, of fax transmission from this peer to the voice gateway for this call. You can derive the Fax Utilization Rate by dividing the FaxTxDuration value by the TxDuration value.
GapFillWithInterpolation	Duration, in ms, of a voice signal played out with a signal synthesized from parameters, or samples of data preceding and following in time because voice data was lost or not received in time from the voice gateway for this call.
GapFillWithRedundancy	Duration, in ms, of a voice signal played out with a signal synthesized from available redundancy parameters because voice data was lost or not received in time from the voice gateway for this call.
GapFillWithPrediction	Duration, in ms, of the voice signal played out with a signal synthesized from parameters, or samples of data preceding in time, because voice data was lost or not received in time from the voice gateway for this call. Examples of such pullout are frame-eraser and frame-concealment strategies in G.729 and G.723.1 compression algorithms.
GapFillWithSilence	Duration, in ms, of a voice signal replaced with silence because voice data was lost or not received in time for this call.
GENERIC	Generic or common parameters; that is, parameters that are common for VoIP and telephony call legs.
H320CallType	Total H320 call types available.
H323 call-legs	Total H.323 call legs for which call records are available.
HiWaterPlayoutDelay	High-water-mark voice playout first in first out (FIFO) delay during this call, in ms.

Table 134 show call active voice Field Descriptions

Field	Description
Index	Dial peer identification number.
InfoActivity	Active information transfer activity state for this call.
InfoType	Information type for this call; for example, voice, speech, or fax.
InSignalLevel	Active input signal level from the telephony interface used by this call.
LogicalIfIndex	Index number of the logical interface for this call.
LoWaterPlayoutDelay	Low-water-mark voice playout FIFO delay during this call, in ms.
Media	Medium over which the call is carried. If the call is carried over the (telephone) access side, the entry is TELE. If the call is carried over the voice network side, the entry is either ATM, Frame Relay (FR), or High-Level Data Link Control (HDLC).
Multicast call-legs	Total multicast call legs for which call records are available.
NoiseLevel	Active noise level for this call.
OnTimeRvPlayout	Duration of voice playout from data received on time for this call. Derive the Total Voice Playout Duration for Active Voice by adding the OnTimeRvPlayout value to the GapFill values.
OutSignalLevel	Active output signal level to the telephony interface used by this call.
PeerAddress	Destination pattern or number associated with this peer.
PeerId	ID value of the peer table entry to which this call was made.
PeerIfIndex	Voice port index number for this peer. For ISDN media, this would be the index number of the B channel used for this call.
PeerSubAddress	Subaddress when this call is connected.
ReceiveBytes	Number of bytes received by the peer during this call.
ReceiveDelay	Average playout FIFO delay plus the decoder delay during this voice call, in ms.
ReceivePackets	Number of packets received by this peer during this call.
RemoteIPAddress	Remote system IP address for the VoIP call.
RemoteUDPPort	Remote system User Datagram Protocol (UDP) listener port to which voice packets are sent.
RoundTripDelay	Voice packet round-trip delay, in ms, between the local and remote systems on the IP backbone for this call.
SCCP call-legs	Call legs for SCCP telephony endpoints.
SelectedQoS	Selected Resource Reservation Protocol (RSVP) quality of service (QoS) for this call.
SessionProtocol	Session protocol used for an Internet call between the local and remote routers through the IP backbone.
SessionTarget	Session target of the peer used for this call.
SetupTime	Value of the system UpTime, in ms, when the call associated with this entry was started.
SIP call-legs	Total SIP call legs for which call records are available.

Table 134 show call active voice Field Descriptions

Field	Description
Telephony call-legs	Total telephony call legs for which call records are available.
Total call-legs	Total number of call legs for the call.
TransmitBytes	Number of bytes sent by this peer during this call.
TransmitPackets	Number of packets sent by this peer during this call.
TxDuration	The length of the call. Appears only if the medium is TELE.
VAD	Whether voice activation detection (VAD) was enabled for this call.
VoiceTxDuration	Duration of voice transmission from this peer to the voice gateway for this call, in ms. Derive the Voice Utilization Rate by dividing the VoiceTxDuration value by the TxDuration value.

The following is sample output from the **show call active voice** command for voice traffic over call-agent controlled call legs. Note that call legs for SCCP telephony endpoints, that is, phones controlled by STCAPP, are displayed under the "Call agent controlled call-legs" field ("SCCP call-legs" displays call legs for devices that are not telephony endpoints; for example, transcoding and conferencing).

```
Router# show call active voice

Telephony call-legs: 2
SIP call-legs: 0
H323 call-legs: 0
Call agent controlled call-legs: 2
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 4

 GENERIC:
SetupTime=1557650 ms
Index=1
PeerAddress=
PeerSubAddress=
PeerId=999100
PeerIfIndex=14
LogicalIfIndex=10
ConnectTime=1562040 ms
CallDuration=00:01:01 sec
CallState=4
CallOrigin=2
ChargedUnits=0
InfoType=speech
TransmitPackets=3101
TransmitBytes=519564
ReceivePackets=3094
ReceiveBytes=494572
TELE:
ConnectionId=[0x11B1860C 0x22D711D7 0x8014E4D4 0x8FD15327]
IncomingConnectionId=[0x11B1860C 0x22D711D7 0x8014E4D4 0x8FD15327]
CallID=25
Port=3/0/0 (25)
BearerChannel=3/0/0.1
TxDuration=59670 ms
VoiceTxDuration=59670 ms
FaxTxDuration=0 ms
CoderTypeRate=g711ulaw
```

```
NoiseLevel=-12
ACOMLevel=22
OutSignalLevel=-12
InSignalLevel=-11
InfoActivity=1
ERLLevel=22
EchoCancellerMaxReflector=2
SessionTarget=
ImgPages=0
CallerName=
CallerIDBlocked=False
OriginalCallingNumber=
OriginalCallingOctet=0x0
OriginalCalledNumber=
OriginalCalledOctet=0x80
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0x0
TranslatedCallingNumber=
TranslatedCallingOctet=0x0
TranslatedCalledNumber=
TranslatedCalledOctet=0x80
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0x0
DSPIdentifier=1/1:1

 GENERIC:
SetupTime=1559430 ms
Index=1
PeerAddress=7702
PeerSubAddress=
PeerId=999100
PeerIfIndex=14
LogicalIfIndex=11
ConnectTime=1562020 ms
CallDuration=00:01:03 sec
CallState=4
CallOrigin=1
ChargedUnits=0
InfoType=speech
TransmitPackets=3151
TransmitBytes=528900
ReceivePackets=3158
ReceiveBytes=503876
TELE:
ConnectionId=[0x0 0x0 0x0 0x0]
IncomingConnectionId=[0x0 0x0 0x0 0x0]
CallID=26
Port=3/0/0 (26)
BearerChannel=3/0/0.2
TxDuration=60815 ms
VoiceTxDuration=60815 ms
FaxTxDuration=0 ms
CoderTypeRate=g711ulaw
NoiseLevel=-12
ACOMLevel=28
OutSignalLevel=-12
InSignalLevel=-11
InfoActivity=1
ERLLevel=28
EchoCancellerMaxReflector=2
SessionTarget=
ImgPages=0
CallerName=
CallerIDBlocked=False
```

```
AlertTimepoint=1559430 ms
OriginalCallingNumber=
OriginalCallingOctet=0x0
OriginalCalledNumber=
OriginalCalledOctet=0x0
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0x0
TranslatedCallingNumber=7701
TranslatedCallingOctet=0x0
TranslatedCalledNumber=7702
TranslatedCalledOctet=0x0
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0x0
GwOutpulsedCalledNumber=7702
GwOutpulsedCalledOctet3=0x0
GwOutpulsedCallingNumber=7701
GwOutpulsedCallingOctet3=0x0
GwOutpulsedCallingOctet3a=0x0
DSPIdentifier=1/1:2

 GENERIC:
SetupTime=1562040 ms
Index=1
PeerAddress=
PeerSubAddress=
PeerId=0
PeerIfIndex=0
LogicalIfIndex=0
ConnectTime=0 ms
CallDuration=00:00:00 sec
CallState=2
CallOrigin=1
ChargedUnits=0
InfoType=speech
TransmitPackets=3215
TransmitBytes=512996
ReceivePackets=3208
ReceiveBytes=512812
VOIP:
ConnectionId[0x0 0x0 0x0 0x0]
IncomingConnectionId[0x0 0x0 0x0 0x0]
CallID=27
RemoteIPAddress=10.10.0.0
RemoteUDPPort=17718
RemoteSignallingIPAddress=10.10.0.0
RemoteSignallingPort=0
RemoteMediaIPAddress=10.2.6.10
RemoteMediaPort=17718
RoundTripDelay=0 ms
SelectedQoS=best-effort
tx_DtmfRelay=inband-voice
FastConnect=FALSE

AnnexE=FALSE

Separate H245 Connection=FALSE

H245 Tunneling=FALSE

SessionProtocol=other
ProtocolCallId=
SessionTarget=
OnTimeRvPlayout=60640
GapFillWithSilence=0 ms
```

```
GapFillWithPrediction=0 ms
GapFillWithInterpolation=0 ms
GapFillWithRedundancy=0 ms
HiWaterPlayoutDelay=105 ms
LoWaterPlayoutDelay=105 ms
TxPakNumber=3040
TxSignalPak=0
TxComfortNoisePak=0
TxDuration=60815
TxVoiceDuration=60815
RxPakNumber=3035
RxSignalPak=0
RxDuration=0
TxVoiceDuration=60690
VoiceRxDuration=60640
RxOutOfSeq=0
RxLatePak=0
RxEarlyPak=0
PlayDelayCurrent=105
PlayDelayMin=105
PlayDelayMax=105
PlayDelayClockOffset=-1662143961
PlayDelayJitter=0
PlayErrPredictive=0
PlayErrInterpolative=0
PlayErrSilence=0
PlayErrBufferOverFlow=0
PlayErrRetroactive=0
PlayErrTalkspurt=0
OutSignalLevel=-12
InSignalLevel=-11
LevelTxPowerMean=0
LevelRxPowerMean=-115
LevelBgNoise=0
ERLLevel=28
ACOMLevel=28
ErrRxDrop=0
ErrTxDrop=0
ErrTxControl=0
ErrRxControl=0
PlayoutMode = undefined
PlayoutInitialDelay=0 ms
ReceiveDelay=105 ms
LostPackets=0
EarlyPackets=0
LatePackets=0
SRTP = off
VAD = disabled
CoderTypeRate=g711ulaw
CodecBytes=160
Media Setting=flow-around

Modem passthrough signaling method is nse:
Buffer Fill Events = 0
Buffer Drain Events = 0
Percent Packet Loss = 0
Consecutive-packets-lost Events = 0
Corrected packet-loss Events = 0
Last Buffer Drain/Fill Event = 0sec
Time between Buffer Drain/Fills = Min 0sec Max 0sec

CallerName=
CallerIDBlocked=False
OriginalCallingNumber=
```

```
OriginalCallingOctet=0x0
OriginalCalledNumber=
OriginalCalledOctet=0x0
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0x0
TranslatedCallingNumber=
TranslatedCallingOctet=0x0
TranslatedCalledNumber=
TranslatedCalledOctet=0x0
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0x0
MediaInactiveDetected=no
MediaInactiveTimestamp=
MediaControlReceived=
Username=

 GENERIC:
SetupTime=1562040 ms
Index=2
PeerAddress=
PeerSubAddress=
PeerId=0
PeerIfIndex=0
LogicalIfIndex=0
ConnectTime=0 ms
CallDuration=00:00:00 sec
CallState=2
CallOrigin=1
ChargedUnits=0
InfoType=speech
TransmitPackets=3380
TransmitBytes=540332
ReceivePackets=3386
ReceiveBytes=540356
VOIP:
ConnectionId[0x0 0x0 0x0 0x0]
IncomingConnectionId[0x0 0x0 0x0 0x0]
CallID=28
RemoteIPAddress=10.0.0.0
RemoteUDPPort=18630
RemoteSignallingIPAddress=10.10.0.0
RemoteSignallingPort=0
RemoteMediaIPAddress=10.2.6.10
RemoteMediaPort=18630
RoundTripDelay=0 ms
SelectedQoS=best-effort
tx_DtmfRelay=inband-voice
FastConnect=FALSE

AnnexE=FALSE

Separate H245 Connection=FALSE

H245 Tunneling=FALSE

SessionProtocol=other
ProtocolCallId=
SessionTarget=
OnTimeRvPlayout=63120
GapFillWithSilence=0 ms
GapFillWithPrediction=0 ms
GapFillWithInterpolation=0 ms
GapFillWithRedundancy=0 ms
HiWaterPlayoutDelay=105 ms
```

```
LoWaterPlayoutDelay=105 ms
TxPakNumber=3158
TxSignalPak=0
TxComfortNoisePak=0
TxDuration=63165
TxVoiceDuration=63165
RxPakNumber=3164
RxSignalPak=0
RxDuration=0
TxVoiceDuration=63165
VoiceRxDuration=63120
RxOutOfSeq=0
RxLatePak=0
RxEarlyPak=0
PlayDelayCurrent=105
PlayDelayMin=105
PlayDelayMax=105
PlayDelayClockOffset=957554296
PlayDelayJitter=0
PlayErrPredictive=0
PlayErrInterpolative=0
PlayErrSilence=0
PlayErrBufferOverFlow=0
PlayErrRetroactive=0
PlayErrTalkspurt=0
OutSignalLevel=-12
InSignalLevel=-11
LevelTxPowerMean=0
LevelRxPowerMean=-114
LevelBgNoise=0
ERLLevel=22
ACOMLevel=22
ErrRxDrop=0
ErrTxDrop=0
ErrTxControl=0
ErrRxControl=0
PlayoutMode = undefined
PlayoutInitialDelay=0 ms
ReceiveDelay=105 ms
LostPackets=0
EarlyPackets=0
LatePackets=0
SRTP = off
VAD = disabled
CoderTypeRate=g711ulaw
CodecBytes=160
Media Setting=flow-around

Modem passthrough signaling method is nse:
Buffer Fill Events = 0
Buffer Drain Events = 0
Percent Packet Loss = 0
Consecutive-packets-lost Events = 0
Corrected packet-loss Events = 0
Last Buffer Drain/Fill Event = 0sec
Time between Buffer Drain/Fills = Min 0sec Max 0sec

CallerName=
CallerIDBlocked=False
OriginalCallingNumber=
OriginalCallingOctet=0x0
OriginalCalledNumber=
OriginalCalledOctet=0x0
OriginalRedirectCalledNumber=
```

```
OriginalRedirectCalledOctet=0x0
TranslatedCallingNumber=
TranslatedCallingOctet=0x0
TranslatedCalledNumber=
TranslatedCalledOctet=0x0
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0x0
MediaInactiveDetected=no
MediaInactiveTimestamp=
MediaControlReceived=
Username=
Telephony call-legs: 2
SIP call-legs: 0
H323 call-legs: 0
Call agent controlled call-legs: 2
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 4
```

Table 132 on page 1727 and Table 134 on page 1732 describe the significant fields shown in the display, in alphabetical order.

The following is sample output from the **show call active voice** command to indicate if Service Advertisement Framework (SAF) is being used:

```
Router# show call active voice

Total call-legs: 2
GENERIC:
SetupTime=1971780 ms
Index=1
PeerAddress=6046692010
PeerSubAddress=
PeerId=20003
PeerIfIndex=17
.
.
.
VOIP:
SessionProtocol=sipv2
ProtocolCallId=7A9E7D9A-EAD311DC-8036BCC4-6EEE85D6@1.5.6.12
SessionTarget=1.5.6.10
SafEnabled=TRUE
SafTrunkRouteId=1
SafPluginDialpeerTag=8
```

Table 132 on page 1727 and Table 136 on page 1744 describe the significant fields shown in the display.

The following is sample output from the **show call active voice** command for fax-relay traffic:

```
Router# show call active voice

Telephony call-legs: 0
SIP call-legs: 0
H323 call-legs: 1
MGCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 1

 GENERIC:
SetupTime=1049400 ms
Index=2
PeerAddress=52930
PeerSubAddress=
```

```
PeerId=82
PeerIfIndex=222
LogicalIfIndex=0
ConnectTime=105105
CallDuration=00:00:59
CallState=4
CallOrigin=1
ChargedUnits=0
InfoType=10
TransmitPackets=1837
TransmitBytes=29764
ReceivePackets=261
ReceiveBytes=4079
VOIP:
ConnectionId[0xEB630F4B 0x9F5E11D7 0x8008CF18 0xB9C3632]
IncomingConnectionId[0xEB630F4B 0x9F5E11D7 0x8008CF18 0xB9C3632]
RemoteIPAddress=10.7.95.3
RemoteUDPPort=16610
RemoteSignallingIPAddress=10.7.95.3
RemoteSignallingPort=1720
RemoteMediaIPAddress=10.7.95.3
RemoteMediaPort=16610
RoundTripDelay=13 ms
SelectedQoS=best-effort
tx_DtmfRelay=inband-voice
FastConnect=TRUE

AnnexE=FALSE

Separate H245 Connection=FALSE

H245 Tunneling=TRUE

SessionProtocol=cisco
ProtocolCallId=
SessionTarget=ipv4:10.7.95.3
OnTimeRvPlayout=1000
GapFillWithSilence=0 ms
GapFillWithPrediction=0 ms
GapFillWithInterpolation=0 ms
GapFillWithRedundancy=0 ms
HiWaterPlayoutDelay=110 ms
LoWaterPlayoutDelay=70 ms
ReceiveDelay=70 ms
LostPackets=0
EarlyPackets=1
LatePackets=0
VAD = enabled
CoderTypeRate=t38
CodecBytes=40
Media Setting=flow-through
AlertTimepoint=104972
CallerName=
CallerIDBlocked=False
OriginalCallingNumber=4085550130
OriginalCallingOctet=0x0
OriginalCalledNumber=52930
OriginalCalledOctet=0xE9
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0x7F
TranslatedCallingNumber=4085550130
TranslatedCallingOctet=0x0
TranslatedCalledNumber=52930
TranslatedCalledOctet=0xE9
```

```
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0xFF
GwReceivedCalledNumber=52930
GwReceivedCalledOctet3=0xE9
GwOutpulsedCalledNumber=52930
GwOutpulsedCalledOctet3=0xE9
GwReceivedCallingNumber=555-0100
GwReceivedCallingOctet3=0x0
GwReceivedCallingOctet3a=0x80
GwOutpulsedCallingNumber=555-0101
GwOutpulsedCallingOctet3=0x0
GwOutpulsedCallingOctet3a=0x80
Username=
FaxRelayMaxJitterBufDepth  = 0 ms
FaxRelayJitterBufOverFlow = 0
FaxRelayHSmodulation = 0
FaxRelayNumberOfPages = 0
Telephony call-legs: 0
SIP call-legs: 0
H323 call-legs: 1
MGCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 1
```

Table 132 on page 1727 and Table 136 on page 1744 describe the significant fields shown in the display.

The following is sample output from the **show call active voice brief** command:

```
Router# show call active voice brief

<ID>: <CallID> <start>hs.<index> +<connect> pid:<peer_id> <dir> <addr> <state>
dur hh:mm:ss tx:<packets>/<bytes> rx:<packets>/<bytes>
IP <ip>:<udp> rtt:<time>ms pl:<play>/<gap>ms lost:<lost>/<early>/<late>
delay:<last>/<min>/<max>ms <codec>
media inactive detected:<y/n> media cntrl rcvd:<y/n> timestamp:<time>
long_duration_call_detected:<y/n> long duration call duration:n/a timestamp:n/a
MODEMPASS <method> buf:<fills>/<drains> loss <overall%> <multipkt>/<corrected>
last <buf event time>s dur:<Min>/<Max>s
FR <protocol> [int dlci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
<codec> (payload size)
ATM <protocol> [int vpi/vci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
<codec> (payload size)
Tele <int> (callID) [channel_id] tx:<tot>/<v>/<fax>ms <codec> noise:<l> acom:<l>
i/o:<l>/<l> dBm
MODEMRELAY info:<rcvd>/<sent>/<resent> xid:<rcvd>/<sent> total:<rcvd>/<sent>/<drops>
speeds(bps): local <rx>/<tx> remote <rx>/<tx>
Proxy <ip>:<audio udp>,<video udp>,<tcp0>,<tcp1>,<tcp2>,<tcp3> endpt: <type>/<manf>
bw: <req>/<act> codec: <audio>/<video>
tx: <audio pkts>/<audio bytes>,<video pkts>/<video bytes>,<t120 pkts>/<t120 bytes>
rx: <audio pkts>/<audio bytes>,<video pkts>/<video bytes>,<t120 pkts>/<t120 bytes>

Total call-legs:2
1269 :7587246hs.1 +260 pid:0 Answer  active
 dur 00:07:14 tx:590/11550 rx:21721/434420
IP 172.29.248.111:17394 rtt:3ms pl:431850/0ms lost:0/0/0 dela
y:69/69/70ms g729r8

1269 :7587246hs.2 +259 pid:133001 Originate 133001 active
 dur 00:07:14 tx:21717/434340 rx:590/11550
 Tele 1/0:1 (2):tx:434350/11640/0ms g729r8 noise:-44 acom:-19
i/0:-45/-45 dBm
```

The following is an example of the **show call active voice** command using the **echo-canceller** keyword. The number 9 represents the hexadecimal ID of an active voice call.

```
Router# show call active voice echo-canceller 9

ACOM=-65  ERL=45
Echo canceller control words=6C 0
Bypass=OFF  Tail=64  Residual ecan=Comfort noise
Freeze=OFF  Modem tone disable=Ignore 2100Hz tone
Worst ERL=6  High level compensation=OFF
Max amplitude reflector (in msec)=5
Ecan version = 8180
```

The following is sample output from the **show call active voice echo-canceller** command for a call with a hexadecimal ID of 10:

```
Router# show call active voice echo-canceller 10

ACOM=-15  ERL=7
Echo canceller control words=6C 0
Bypass=OFF  Tail=64  Residual ecan=Comfort noise
Freeze=OFF  Modem tone disable=Ignore 2100Hz tone
Worst ERL=6  High level compensation=OFF
Max amplitude reflector (in msec)=64
```

The call ID number (which is 10 in the preceding example) changes with every new active call. When an active call is up, you must enter the **show call active voice brief** command to obtain the call ID number. The call ID must be converted to hexadecimal value if you want to use the **show call active voice echo-canceller** *x* command (*x* = call ID converted to hexadecimal value).

Table 135 shows call ID examples converted to hexadecimal values (generally incremented by 2):

Table 135 Call IDs Converted to Hex

Decimal	Hex
2	2
4	4
6	6
8	8
10	A
12	C

Alternatively, you can use the **show voice call status** command to obtain the call ID. The call ID output is already in hexadecimal values form when you use this command:

```
Router# show voice call status

CallID     CID  ccVdb      Port      DSP/Ch  Called #   Codec    Dial-peers
0x1        11CE 0x02407B20 1:0.1     1/1     1000       g711ulaw 2000/1000
```

The following is sample output from the **show call active voice** command using the **compact** keyword:

```
Router# show call active voice compact

<callID>   A/O FAX T<sec> Codec    type    Peer Address    IP R<ip>:<udp>
Total call-legs: 2
58 ANS     T11          g711ulaw   VOIP     Psipp 2001:.....:230A:6080
59 ORG     T11          g711ulaw   VOIP     P5000110011       10.13.37.150:6090
```

The following is sample output from the **show call active voice redirect** command using the **tbct** keyword:

```
Router# show call active voice redirect tbct

TBCT:
        Maximum no. of TBCT calls allowed:No limit
        Maximum TBCT call duration:No limit


Total number TBCT calls currently being monitored = 1

ctrl name=T1-2/0, tag=13, call-ids=(7, 8), start_time=*00:12:25.985 UTC Mon Mar 1 1993
```

Table 136 describes the significant fields shown in the display.

Table 136 show call active voice redirect Field Descriptions

Field	Description
Maximum no. of TBCT calls allowed	Maximum number of calls that can use TBCT as defined by the **tbct max calls** command.
Maximum TBCT call duration	Maximum length allowed for a TBCT call as defined by the **tbct max call-duration** command.
Total number TBCT calls currently being monitored	Total number of active TBCT calls.
ctrl name	Name of the T1 controller where the call originated.
tag	Call tag number that identifies the call.
call-ids	Numbers that uniquely identify the call legs.
start_time	Time, in hours, minutes, and seconds, when the redirected call began.

Related Commands

Command	Description
show call active fax	Displays call information for fax transmissions that are in progress.
show call history	Displays the call history table.
show call-router routes	Displays the dynamic routes in the cache of the BE.
show call-router status	Displays the Annex G BE status.
show dial-peer voice	Displays configuration information for dial peers.
show num-exp	Displays how the number expansions are configured in VoIP.
show voice call status	Displays the call status for voice ports on the Cisco router or concentrator.
show voice port	Displays configuration information about a specific voice port.

show call history fax

To display the call history table for fax transmissions, use the **show call history fax** command in user EXEC or privileged EXEC mode.

show call history fax [**brief** [**id** *identifier*] | **compact** [**duration** {**less** | **more**} *time*] | **id** *identifier* | **last** *number*]

Syntax Description

brief	(Optional) Displays a truncated version of the call history table.
id *identifier*	(Optional) Displays only the call with the specified identifier. Range is a hex value from 1 to FFFF.
compact	(Optional) Displays a compact version.
duration *time*	(Optional) Displays history information for calls that are longer or shorter than a specified *time* value. The arguments and keywords are as follows: • **less**—Displays calls shorter than the value in the *time* argument. • **more**—Displays calls longer than the value in the *time* argument. • *time*—Elapsed time, in seconds. Range is from 1 to 2147483647.
last *number*	(Optional) Displays the last calls connected, where the number of calls that appear is defined by the *number* argument. Range is from 1 to 100.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
12.0(3)XG	This command was implemented for Voice over Frame Relay (VoFR) on the Cisco 2600 series and Cisco 3600 series.
12.0(4)XJ	This command was modified for store-and-forward fax.
12.0(4)T	This command was modified. The **brief** keyword was added, and the command was implemented on the Cisco 7200 series.
12.0(7)XK	This command was modified. The **brief** keyword was implemented on the Cisco MC3810.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(5)XM	This command was implemented on the Cisco AS5800.
12.1(5)XM2	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XA	This command was modified. The output of this command was modified to indicate whether the call in question has been established using Annex E.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 was not included in this release.

Release	Modification
12.2(11)T	This command was implemented on the Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850.
12.3(1)	This command was modified. The following fields were added: FaxRelayMaxJitterBufDepth, FaxRelayJitterBufOverFlow, FaxRelayHSmodulation, and FaxRelayNumberOfPages.
12.3(14)T	This command was modified. 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.
12.4(15)T	This command was modified. The Port and BearerChannel display fields were added to the TELE call leg record of the command output.
12.4(16)	This command was modified. The Port and BearerChannel display fields were added to the TELE call leg record of the command output.
12.4(22)T	This command was modified. Command output was updated to show IPv6 information.

Usage Guidelines

This command displays a call-history table that contains a list of fax calls connected through the router in descending time order. The maximum number of calls contained in the table can be set to a number from 0 to 500 using the **dial-control-mib** command in global configuration mode. The default maximum number of table entries is 50. Each call record is aged out of the table after a configurable number of minutes has elapsed, also specified by the **dial-control-mib** command. The default timer value is 15 minutes.

You can display subsets of the call history table by using specific keywords. To display the last calls connected through this router, use the keyword **last**, and define the number of calls to be displayed with the *number* argument.

To display a truncated version of the call history table, use the **brief** keyword.

This command applies to both on-ramp and off-ramp store-and-forward fax functions.

Examples

The following is sample output from the **show call history fax** command:

```
Router# show call history fax

Telephony call-legs: 1
SIP call-legs: 0
H323 call-legs: 0
MGCP call-legs: 0
Total call-legs: 1


GENERIC:
SetupTime=590180 ms
Index=2
PeerAddress=4085452930
PeerSubAddress=
PeerId=81
PeerIfIndex=221
LogicalIfIndex=145
DisconnectCause=10
DisconnectText=normal call clearing (16)
ConnectTime=59389
DisconnectTime=68204
```

```
CallDuration=00:01:28
CallOrigin=2
ReleaseSource=1
ChargedUnits=0
InfoType=fax
TransmitPackets=295
TransmitBytes=5292
ReceivePackets=2967
ReceiveBytes=82110
TELE:
ConnectionId=[0xD9ACDFF1 0x9F5D11D7 0x8002CF18 0xB9C3632]
IncomingConnectionId=[0xD9ACDFF1 0x9F5D11D7 0x8002CF18 0xB9C3632]
CallID=2
Port=3/0/0 (2)
BearerChannel=3/0/0.1
TxDuration=28960 ms
VoiceTxDuration=0 ms
FaxTxDuration=28960 ms
FaxRate=voice bps
FaxRelayMaxJitterBufDepth  = 0 ms
FaxRelayJitterBufOverFlow = 0
FaxRelayHSmodulation = 0
FaxRelayNumberOfPages = 0
NoiseLevel=-120
ACOMLevel=127
SessionTarget=
ImgPages=0
CallerName=
CallerIDBlocked=False
OriginalCallingNumber=4085550130
OriginalCallingOctet=0x0
OriginalCalledNumber=52930
OriginalCalledOctet=0xE9
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0xFF
TranslatedCallingNumber=4085550130
TranslatedCallingOctet=0x0
TranslatedCalledNumber=52930
TranslatedCalledOctet=0xE9
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0xFF
GwReceivedCalledNumber=52930
GwReceivedCalledOctet3=0xE9
GwReceivedCallingNumber=4085550130
GwReceivedCallingOctet3=0x0
GwReceivedCallingOctet3a=0x80
```

Table 137 provides an alphabetical listing of the fields displayed in the output of the **show call history fax** command and a description of each field.

Table 137 show call history fax Field Descriptions

Field	Description
ACOM Level	Current ACOM level for this call. ACOM is the combined loss achieved by the echo canceler, which is the sum of the Echo Return Loss, Echo Return Loss Enhancement, and nonlinear processing loss for the call.
BearerChannel	Identification of the bearer channel carrying the call.
Buffer Drain Events	Total number of jitter buffer drain events.

Table 137 show call history fax Field Descriptions (continued)

Field	Description
Buffer Fill Events	Total number of jitter buffer fill events.
CallDuration	Length of the call, in hours, minutes, and seconds, hh:mm:ss.
CallerName	Voice port station name string.
CallOrigin	Call origin: answer or originate.
CallState	Current state of the call.
ChargedUnits	Total number of charging units that apply to this peer since system startup. The unit of measure for this field is hundredths of second.
CodecBytes	Payload size, in bytes, for the codec used.
CoderTypeRate	Negotiated coder rate. This value specifies the send rate of voice or fax compression to its associated call leg for this call.
ConnectionId	Global call identifier for this gateway call.
ConnectTime	Time, in milliseconds (ms), at which the call was connected.
Consecutive-packets-lost Events	Total number of consecutive (two or more) packet-loss events.
Corrected packet-loss Events	Total number of packet-loss events that were corrected using the RFC 2198 method.
Dial-Peer	Tag of the dial peer sending this call.
DisconnectCause	Cause code for the reason this call was disconnected.
DisconnectText	Descriptive text explaining the reason for the disconnect.
DisconnectTime	Time, in ms, when this call was disconnected.
EchoCancellerMaxReflector=64	The location of the largest reflector, in ms. The reflector size does not exceed the configured echo path capacity. For example, if 32 ms is configured, the reflector does not report beyond 32 ms.
ERLLevel	Current Echo Return Loss (ERL) level for this call.
FaxTxDuration	Duration of fax transmission from this peer to the voice gateway for this call. You can derive the Fax Utilization Rate by dividing the FaxTxDuration value by the TxDuration value.
FaxRelayJitterBufOverFlow	Count of number of network jitter buffer overflows (number of packets). These packets are equivalent to lost packets.
FaxRelayMaxJitterBufDepth	Maximum depth of jitter buffer (in ms).
FaxRelayHSmodulation	Most recent high-speed modulation used.
FaxRelayNumberOfPages	Number of pages transmitted.
GapFillWithInterpolation	Duration of a voice signal played out with a signal synthesized from parameters, or samples of data preceding and following in time because voice data was lost or not received in time from the voice gateway for this call.
GapFillWithRedundancy	Duration of a voice signal played out with a signal synthesized from available redundancy parameters because voice data was lost or not received in time from the voice gateway for this call.

Table 137 show call history fax Field Descriptions (continued)

Field	Description
GapFillWithPrediction	Duration of the voice signal played out with signal synthesized from parameters, or samples of data preceding in time, because voice data was lost or not received in time from the voice gateway for this call. Examples of such pullout are frame-eraser and frame-concealment strategies in G.729 and G.723.1 compression algorithms.
GapFillWithSilence	Duration of a voice signal replaced with silence because voice data was lost or not received in time for this call.
GENERIC	Generic or common parameters, that is, parameters that are common for VoIP and telephony call legs.
GwReceivedCalledNumber, GwReceivedCalledOctet3, GwReceivedCallingNumber, GwReceivedCallingOctet3, GwReceivedCallingOctet3a	Call information received at the gateway.
H323 call-legs	Total H.323 call legs for which call records are available.
HiWaterPlayoutDelay	High-water-mark Voice Playout FIFO Delay during this call.
ImgPages	The fax pages that have been processed.
Incoming ConnectionId	The incoming_GUID. It can be different with ConnectionId (GUID) when there is a long_pound or blast_call feature involved. In those cases, incoming_GUID is unique for all the subcalls that have been generated, and GUID is different for each subcall.
Index	Dial peer identification number.
InfoActivity	Active information transfer activity state for this call.
InfoType	Information type for this call; for example, voice or fax.
InSignalLevel	Active input signal level from the telephony interface used by this call.
Last Buffer Drain/Fill Event	Elapsed time since the last jitter buffer drain or fill event, in seconds.
LogicalIfIndex	Index number of the logical interface for this call.
LoWaterPlayoutDelay	Low-water-mark Voice Playout FIFO Delay during this call.
LowerIFName	Physical lower interface information. Appears only if the medium is ATM, Frame Relay (FR), or High-Level Data Link Control (HDLC).
Media	Medium over which the call is carried. If the call is carried over the (telephone) access side, the entry is TELE. If the call is carried over the voice network side, the entry is either ATM, FR, or HDLC.

Table 137 show call history fax Field Descriptions (continued)

Field	Description
Modem passthrough signaling method in use	Indicates that this is a modem pass-through call and that named signaling events (NSEs)—a Cisco-proprietary version of named telephone events in RFC 2833—are used for signaling codec upspeed. The upspeed method is the method used to dynamically change the codec type and speed to meet network conditions. This means that you might move to a faster codec when you have both voice and data calls and then slow down when there is only voice traffic.
NoiseLevel	Active noise level for this call.
OnTimeRvPlayout	Duration of voice playout from data received on time for this call. Derive the Total Voice Playout Duration for Active Voice by adding the OnTimeRvPlayout value to the GapFill values.
OriginalCallingNumber, OriginalCalling Octet, OriginalCalledNumber, OriginalCalledOctet, OriginalRedirectCalledNumber, OriginalRedirectCalledOctet	Original call information regarding calling, called, and redirect numbers, as well as octet-3s. Octet-3s are information elements (IEs) of Q.931 that include type of number, numbering plan indicator, presentation indicator, and redirect reason information.
OutSignalLevel	Active output signal level to the telephony interface used by this call.
PeerAddress	Destination pattern or number associated with this peer.
PeerId	ID value of the peer table entry to which this call was made.
PeerIfIndex	Voice port index number for this peer. For ISDN media, this would be the index number of the B channel used for this call.
PeerSubAddress	Subaddress when this call is connected.
Percent Packet Loss	Total percent packet loss.
Port	Identification of the voice port carrying the call.
ReceiveBytes	Number of bytes received by the peer during this call.
ReceiveDelay	Average Playout FIFO Delay plus the Decoder Delay during this voice call.
ReceivePackets	Number of packets received by this peer during this call.
ReleaseSource	Number value of the release source.
RemoteIPAddress	Remote system IP address for the VoIP call.
RemoteUDPPort	Remote system User Datagram Protocol (UDP) listener port to which voice packets are sent.
RoundTripDelay	Voice packet round-trip delay between the local and remote systems on the IP backbone for this call.
SelectedQoS	Selected Resource Reservation Protocol (RSVP) quality of service (QoS) for this call.
SessionProtocol	Session protocol used for an Internet call between the local and remote routers through the IP backbone.
SessionTarget	Session target of the peer used for this call.

Table 137 show call history fax Field Descriptions (continued)

Field	Description
SetupTime	Value of the system UpTime, in ms, when the call associated with this entry was started.
SignalingType	Signaling type for this call; for example, channel-associated signaling (CAS) or common-channel signaling (CCS).
SIP call-legs	Total SIP call legs for which call records are available.
Telephony call-legs	Total telephony call legs for which call records are available.
Time between Buffer Drain/Fills	Minimum and maximum durations between jitter buffer drain or fill events, in seconds.
TranslatedCallingNumber, TranslatedCallingOctet, TranslatedCalledNumber, TranslatedCalledOctet, TranslatedRedirectCalled Number, TranslatedRedirectCalledOctet	Translated call information.
TransmitBytes	Number of bytes sent by this peer during this call.
TransmitPackets	Number of packets sent by this peer during this call.
TxDuration	The length of the call. Appears only if the medium is TELE.
VAD	Whether voice activation detection (VAD) was enabled for this call.
VoiceTxDuration	Duration of voice transmission from this peer to the voice gateway for this call. Derive the Voice Utilization Rate by dividing the VoiceTxDuration value by the TxDuration value.

The following is sample output from the **show call history fax brief** command:

```
Router# show call history fax brief

<ID>: <start>hs.<index> +<connect> +<disc> pid:<peer_id> <direction> <addr>
 tx:<packets>/<bytes> rx:<packets>/<bytes> <disc-cause>(<text>)
 IP <ip>:<udp> rtt:<time>ms pl:<play>/<gap>ms lost:<lost>/<early>/<late>
  delay:<last>/<min>/<max>ms <codec>
 Telephony <int>: tx:<tot>/<voice>/<fax>ms <codec> noise:<lvl>dBm acom:<lvl>dBm

2    : 5996450hs.25 +-1 +3802 pid:100 Answer 408
 tx:0/0 rx:0/0 1F  (T30 T1 EOM timeout)
 Telephony : tx:38020/38020/0ms g729r8 noise:0dBm acom:0dBm

2    : 5996752hs.26 +-1 +3500 pid:110 Originate uut1@linux2.allegro.com
 tx:0/0 rx:0/0 3F  (The e-mail was not sent correctly. Remote SMTP server said: 354 )
 IP 14.0.0.1 AcceptedMime:0 DiscardedMime:0

3    : 6447851hs.27 +1111 +3616 pid:310 Originate 576341.
 tx:11/14419 rx:0/0 10  (Normal connection)
 Telephony : tx:36160/11110/25050ms g729r8 noise:115dBm acom:-14dBm

3    : 6447780hs.28 +1182 +4516 pid:0 Answer
 tx:0/0 rx:0/0 10  (normal call clearing.)
 IP 0.0.0.0 AcceptedMime:0 DiscardedMime:0

4    : 6464816hs.29 +1050 +3555 pid:310 Originate 576341.
```

```
 tx:11/14413 rx:0/0 10  (Normal connection)
 Telephony : tx:35550/10500/25050ms g729r8 noise:115dBm acom:-14dBm

4    : 6464748hs.30 +1118 +4517 pid:0 Answer
 tx:0/0 rx:0/0 10  (normal call clearing.)
 IP 0.0.0.0 AcceptedMime:0 DiscardedMime:0

5    : 6507900hs.31 +1158 +2392 pid:100 Answer 4085763413
 tx:0/0 rx:3/3224 10  (Normal connection)
 Telephony : tx:23920/11580/12340ms g729r8 noise:0dBm acom:0dBm

5    : 6508152hs.32 +1727 +2140 pid:110 Originate uut1@linux2.allegro.com
 tx:0/2754 rx:0/0 3F  (service or option not available, unspecified)
 IP 14.0.0.4 AcceptedMime:0 DiscardedMime:0

6    : 6517176hs.33 +1079 +3571 pid:310 Originate 576341.
 tx:11/14447 rx:0/0 10  (Normal connection)
 Telephony : tx:35710/10790/24920ms g729r8 noise:115dBm acom:-14dBm

6    : 6517106hs.34 +1149 +4517 pid:0 Answer
 tx:0/0 rx:0/0 10  (normal call clearing.)
 IP 0.0.0.0 AcceptedMime:0 DiscardedMime:0

7    : 6567382hs.35 +1054 +3550 pid:310 Originate 576341.
 tx:11/14411 rx:0/0 10  (Normal connection)
 Telephony : tx:35500/10540/24960ms g729r8 noise:115dBm acom:-14dBm

7    : 6567308hs.36 +1128 +4517 pid:0 Answer
tx:0/0 rx:0/0 10  (normal call clearing.)
 IP 0.0.0.0 AcceptedMime:0 DiscardedMime:0
```

The following example shows output for the **show call history fax** command with the T.38 Fax Relay statistics:

```
Router# show call history fax

Telephony call-legs: 1
SIP call-legs: 0
H323 call-legs: 0
MGCP call-legs: 0
Total call-legs: 1


GENERIC:
SetupTime=9872460 ms
Index=8
PeerAddress=41023
PeerSubAddress=
PeerId=1
PeerIfIndex=242
LogicalIfIndex=180
DisconnectCause=10
DisconnectText=normal call clearing (16)
ConnectTime=9875610 ms
DisconnectTime=9936000 ms
CallDuration=00:01:00 sec
CallOrigin=2
ReleaseSource=1
ChargedUnits=0
InfoType=fax
TransmitPackets=268
TransmitBytes=4477
ReceivePackets=1650
ReceiveBytes=66882
```

```
TELE:
ConnectionId=[0xD6635DD5 0x9FA411D8 0x8005000A 0xF4107CA0]
IncomingConnectionId=[0xD6635DD5 0x9FA411D8 0x8005000A 0xF4107CA0]
CallID=7
Port=3/0/0:0 (7)
BearerChannel=3/0/0.8
TxDuration=6170 ms
VoiceTxDuration=0 ms
FaxTxDuration=0 ms
FaxRate=disable bps
FaxRelayMaxJitterBufDepth=560 ms
FaxRelayJitterBufOverFlow=0
FaxRelayMostRecentHSmodulation=V.17/short/14400
FaxRelayNumberOfPages=1
FaxRelayInitHSmodulation=V.17/long/14400
FaxRelayDirection=Transmit
FaxRelayPktLossConceal=0
FaxRelayEcmStatus=ENABLED
FaxRelayEncapProtocol=T.38 (UDPTL)
FaxRelayNsfCountryCode=Japan
FaxRelayNsfManufCode=0031B8EE80C48511DD0D0000DDDD0000DDDD00000000000000000022ED00B0A400
FaxRelayFaxSuccess=Success
NoiseLevel=0
ACOMLevel=0
SessionTarget=
ImgPages=0
CallerName=Analog 41023
CallerIDBlocked=False
OriginalCallingNumber=
OriginalCallingOctet=0x80
OriginalCalledNumber=41021
OriginalCalledOctet=0xA1
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0xFF
TranslatedCallingNumber=41023
TranslatedCallingOctet=0x80
TranslatedCalledNumber=41021
TranslatedCalledOctet=0xA1
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0xFF
GwReceivedCalledNumber=41021
GwReceivedCalledOctet3=0xA1
```

Table 138 describes the fields not shown in Table 137.

Table 138 show call history fax Field Descriptions

Field	Description
FaxRelayDirection	Direction of fax relay.
FaxRelayEcmStatus	Fax relay error correction mode status.
FaxRelayEncapProtocol	Fax relay encapsulation protocol.
FaxRelayFaxSuccess	Fax relay success.
FaxRelayInitHSmodulation	Fax relay initial high speed modulation.
FaxRelayMostRecentHSmodulation	Fax relay most recent high speed modulation.
FaxRelayNsfCountryCode	Fax relay Nonstandard Facilities (NSF) country code.
FaxRelayNsfManufCode	Fax relay NSF manufacturers code.
FaxRelayPktLossConceal	Fax relay packet loss conceal.

Related Commands

Command	Description
dial-control-mib	Specifies attributes for the call history table.
show call active fax	Displays call information for fax transmissions that are in progress.
show call active voice	Displays call information for voice calls that are in progress.
show call history voice	Displays the call history table for voice calls.
show dial-peer voice	Displays configuration information for dial peers.
show num-exp	Displays how the number expansions are configured in VoIP.
show voice port	Displays configuration information about a specific voice port.

show call history voice

To display the call history table for voice calls, use the **show call history voice** command in user EXEC or privileged EXEC mode.

show call history voice [**brief** [**id** *identifier*] | **compact** [**duration** {**less** | **more**} *seconds*] | **id** *identifier* | **last** *number* | **redirect** {**rtpvt** | **tbct**} | **stats**]

Syntax Description

brief	(Optional) Displays a truncated version of the call history table.
id *identifier*	(Optional) Displays only the call with the specified identifier. Range is from 1 to FFFF.
compact	(Optional) Displays a compact version of the call history table.
duration *seconds*	(Optional) Displays history information for calls that are longer or shorter than the value of the specified *seconds* argument. The arguments and keywords are as follows: • **less**—Displays calls shorter than the *seconds* value. • **more**—Displays calls longer than the *seconds* value. • *seconds*—Elapsed time, in seconds. Range is from 1 to 2147483647.
last *number*	(Optional) Displays the last calls connected, where the number of calls that appear is defined by the *number* argument. Range is from 1 to 100.
redirect	(Optional) Displays information about calls that were redirected using Release-to-Pivot (RTPvt) or Two B-Channel Transfer (TBCT). The keywords are as follows: • **rtpvt**—Displays information about RTPvt calls. • **tbct**—Displays information about TBCT calls.
stats	(Optional) Displays information about digital signal processing (DSP) voice quality metrics.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
12.0(3)XG	Support was added for Voice over Frame Relay (VoFR) on the Cisco 2600 series and Cisco 3600 series.
12.0(4)XJ	This command was modified for store-and-forward fax.
12.0(4)T	The **brief** keyword was added, and the command was implemented on the Cisco 7200 series.
12.0(5)XK	This command was implemented on the Cisco MC3810.
12.0(7)XK	The **brief** keyword was implemented on the Cisco MC3810.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Release	Modification
12.1(5)XM	This command was implemented on the Cisco AS5800.
12.1(5)XM2	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XA	The output of this command was modified to indicate whether a specified call has been established using Annex E.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support was not included for the Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850.
12.2(11)T	Support was added for Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850.
12.2(13)T	The ReleaseSource field was added to the Field Description table, and the **record** keyword was deleted from the command name.
12.3(1)	The **redirect** keyword was added.
12.4(2)T	The LocalHostname display field was added to the VoIP call leg record.
12.4(11)XW	The **stats** keyword was added.
12.4(15)T	The Port and BearerChannel display fields were added to the TELE call leg record of the command output.
12.4(16)	The Port and BearerChannel display fields were added to the TELE call leg record of the command output.
12.4(22)T	Command output was updated to show IPv6 information.

Usage Guidelines

This command displays a call-history table that contains a list of voice calls connected through the router in descending time order. The maximum number of calls contained in the table can be set to a number from 0 to 500 using the **dial-control-mib** command in global configuration mode. The default maximum number of table entries is 50. Each call record is aged out of the table after a configurable number of minutes has elapsed. The timer value is also specified by the **dial-control-mib** command. The default timer value is 15 minutes.

You can display subsets of the call history table by using specific keywords. To display the last calls connected through this router, use the **last** keyword, and define the number of calls to be displayed with the *number* argument.

To display a truncated version of the call history table, use the **brief** keyword.

Use the **show call active voice redirect** command to review records for calls that implemented RTPvt or TBCT.

When a call is active, you can display its statistics by using the **show call active voice** command.

Examples

The following is sample output from the **show call history voice** command:

```
Router# show call history voice

GENERIC:
SetupTime=104648 ms
Index=1
PeerAddress=55240
PeerSubAddress=
```

```
PeerId=2
PeerIfIndex=105
LogicalIfIndex=0
DisconnectCause=10
DisconnectText=normal call clearing.
ConnectTime=104964
DisconectTime=143329
CallDuration=00:06:23
CallOrigin=1
ChargedUnits=0
InfoType=speech
TransmitPackets=37668
TransmitBytes=6157536
ReceivePackets=37717
ReceiveBytes=6158452
VOIP:
ConnectionId[0x4B091A27 0x3EDD0003 0x0 0xFEFD4]
CallID=2
RemoteIPAddress=10.14.82.14
RemoteUDPPort=18202
RoundTripDelay=2 ms
SelectedQoS=best-effort
tx_DtmfRelay=inband-voice
FastConnect=TRUE

SessionProtocol=cisco
SessionTarget=ipv4:10.14.82.14
OnTimeRvPlayout=40
GapFillWithSilence=0 ms
GapFillWithPrediction=0 ms
GapFillWithInterpolation=0 ms
GapFillWithRedundancy=0 ms
HiWaterPlayoutDelay=67 ms
LoWaterPlayoutDelay=67 ms
ReceiveDelay=67 ms
LostPackets=0 ms
EarlyPackets=0 ms
LatePackets=0 ms
VAD = enabled
CoderTypeRate=g729r8
CodecBytes=20
cvVoIPCallHistoryIcpif=0
SignalingType=cas

Modem passthrough signaling method is nse
Buffer Fill Events = 0
Buffer Drain Events = 0
Percent Packet Loss = 0
Consecutive-packets-lost Events = 0
Corrected packet-loss Events = 0
Last Buffer Drain/Fill Event = 373sec
Time between Buffer Drain/Fills = Min 0sec Max 0sec

GENERIC:
SetupTime=104443 ms
Index=2
PeerAddress=50110
PeerSubAddress=
PeerId=100
PeerIfIndex=104
LogicalIfIndex=10
DisconnectCause=10
DisconnectText=normal call clearing.
ConnectTime=104964
```

```
DisconectTime=143330
CallDuration=00:06:23
CallOrigin=2
ChargedUnits=0
InfoType=speech
TransmitPackets=37717
TransmitBytes=5706436
ReceivePackets=37668
ReceiveBytes=6609552
TELE:
ConnectionId=[0x4B091A27 0x3EDD0003 0x0 0xFEFD4]
CallID=3
Port=3/0/0 (3)
BearerChannel=3/0/0.1
TxDuration=375300 ms
VoiceTxDuration=375300 ms
FaxTxDuration=0 ms
CoderTypeRate=g711ulaw
NoiseLevel=-75
ACOMLevel=11
SessionTarget=
ImgPages=0
```

The following example from a Cisco AS5350 router displays a sample of voice call history records showing release source information:

```
Router# show call history voice

Telephony call-legs: 1
SIP call-legs: 0
H323 call-legs: 1
Total call-legs: 2

GENERIC:
SetupTime=85975291 ms
.
.
.
DisconnectCause=10
DisconnectText=normal call clearing (16)
ConnectTime=85975335
DisconnectTime=85979339
CallDuration=00:00:40
CallOrigin=1
ReleaseSource=1
.

.
.
DisconnectCause=10
DisconnectText=normal call clearing (16)
ConnectTime=85975335
DisconnectTime=85979339
CallDuration=00:00:40
CallOrigin=1
ReleaseSource=1
.
.
.
VOIP:
ConnectionId[0x2868AD84 0x375B11D4 0x8012F7A5 0x74DE971E]
CallID=1
.
.
```

```
.
GENERIC:
SetupTime=85975290 ms
.
.
.
DisconnectCause=10
DisconnectText=normal call clearing (16)
ConnectTime=85975336
DisconnectTime=85979340
CallDuration=00:00:40
CallOrigin=2
ReleaseSource=1
.
.
.
TELE:
ConnectionId=[0x2868AD84 0x375B11D4 0x8012F7A5 0x74DE971E]
CallID=2
Port=3/0/0 (2)
BearerChannel=3/0/0.1
```

The following is sample output from the **show call history voice brief** command:

```
Router# show call history voice brief

<ID>: <CallID> <start>hs.<index> +<connect> +<disc> pid:<peer_id> <direction> <addr>
dur hh:mm:ss tx:<packets>/<bytes> rx:<packets>/<bytes> <disc-cause>(<text>)
IP <ip>:<udp> rtt:<time>ms pl:<play>/<gap>ms lost:<lost>/<early>/<late>
delay:<last>/<min>/<max>ms <codec>
media inactive detected:<y/n> media cntrl rcvd:<y/n> timestamp:<time>
MODEMPASS <method> buf:<fills>/<drains> loss <overall%> <multipkt>/<corrected>
last <buf event time>s dur:<Min>/<Max>s
FR <protocol> [int dlci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
<codec> (payload size)
ATM <protocol> [int vpi/vci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
<codec> (payload size)
Telephony <int> (callID) [channel_id] tx:<tot>/<voice>/<fax>ms <codec> noise:<lvl>dBm
acom:<lvl>dBm
MODEMRELAY info:<rcvd>/<sent>/<resent> xid:<rcvd>/<sent> total:<rcvd>/<sent>/<drops>
disc:<cause code>
speeds(bps): local <rx>/<tx> remote <rx>/<tx>
Proxy <ip>:<audio udp>,<video udp>,<tcp0>,<tcp1>,<tcp2>,<tcp3> endpt: <type>/<manf>
bw: <req>/<act> codec: <audio>/<video>
tx: <audio pkts>/<audio bytes>,<video pkts>/<video bytes>,<t120 pkts>/<t120 bytes>
rx: <audio pkts>/<audio bytes>,<video pkts>/<video bytes>,<t120 pkts>/<t120 bytes>
```

The following is sample output from the **show call history voice redirect** command:

```
Router# show call history voice redirect tbct

index=2, xfr=tbct-notify, status=redirect_success, start_time=*00:12:25.981 UTC Mon Mar 1
1993, ctrl name=T1-2/0,  tag=13
index=3, xfr=tbct-notify, status=redirect_success, start_time=*00:12:25.981 UTC Mon Mar 1
1993, ctrl name=T1-2/0,  tag=13
index=4, xfr=tbct-notify, status=redirect_success, start_time=*00:13:07.091 UTC Mon Mar 1
1993, ctrl name=T1-2/0,  tag=12
index=5, xfr=tbct-notify, status=redirect_success, start_time=*00:13:07.091 UTC Mon Mar 1
1993, ctrl name=T1-2/0,  tag=12

Number of call-legs redirected using tbct with notify:4
```

Table 139 describes the significant fields shown in the **show call history voice redirect tbct** display.

Table 139 show call history voice redirect Field Descriptions

Field	Description
index	Index number of the record in the history file.
xfr	Whether TBCT or TBCT with notify has been invoked.
status	Status of the redirect request.
start_time	Time, in hours, minutes, and seconds when the redirected call began.
ctrl name	Name of the T1 controller where the call originated.
tag	Call tag number that identifies the call.
Number of call-legs redirected using tbct with notify	Total number of call legs that were redirected using TBCT with notify.

Related Commands

Command	Description
dial-control-mib	Set the maximum number of calls contained in the table.
show call active fax	Displays call information for fax transmissions that are in progress.
show call active voice	Displays call information for voice calls that are in progress.
show call history fax	Displays the call history table for fax transmissions.
show dial-peer voice	Displays configuration information for dial peers.
show num-exp	Displays how the number expansions are configured in VoIP.
show voice port	Displays configuration information about a specific voice port.

show cdp entry

To display information about a specific neighboring device discovered using Cisco Discovery Protocol (CDP), use the **show cdp entry** command in privileged EXEC mode.

show cdp entry {***** | *device-name*[*****]} [**version**] [**protocol**]

Syntax Description

*****	Displays all of the CDP neighbors.
device-name[*****]	Name of the neighbor about which you want information. You can enter an optional asterisk (*) at the end of a *device-name* as a wildcard. For example, entering **show cdp entry dev*** will match all device names that begin with **dev**.
version	(Optional) Limits the display to information about the version of software running on the router.
protocol	(Optional) Limits the display to information about the protocols enabled on a router.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.2(8)T	Support for IPv6 address and address type information was added.
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.
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.
12.2SX	This command is supported in the Cisco 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 cdp entry** command. Information about the neighbor *device.cisco.com* is displayed, including device ID, protocols and addresses, platform, interface, hold time, and version.

```
Router# show cdp entry device.cisco.com

Device ID: device.cisco.com
Entry address(es):
  IP address: 10.1.17.24
  IPv6 address: FE80::203:E3FF:FE6A:BF81  (link-local)
  IPv6 address: 4000::BC:0:0:C0A8:BC06  (global unicast)
  CLNS address: 490001.1111.1111.1111.00
Platform: cisco 3640,  Capabilities: Router
Interface: Ethernet0/1,  Port ID (outgoing port): Ethernet0/1
Holdtime : 160 sec

Version :
```

```
Cisco Internetwork Operating System Software
IOS (tm) 3600 Software (C3640-A2IS-M), Experimental Version 12.2
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Wed 08-Aug-01 12:39 by joeuser
```

Table 140 describes the significant fields shown in the example.

Table 140 show cdp entry Field Descriptions

Field	Definition
Device ID: device.cisco.com	Name or ID of the device.
Entry address(es):	The IP, IPv6 link-local, IPv6 global unicast, and CLNS addresses.
Platform:	Platform information specific to the device.
Interface: Ethernet0/1, Port ID (outgoing port): Ethernet0/1	Information about the interface and port ID interface.
Holdtime:	Holdtime length in seconds.
Version:	Information about the software version.

The following is sample output from the **show cdp entry version** command. Only information about the version of software running on *device.cisco.com* is displayed.

```
Router# show cdp entry device.cisco.com version

Version information for device.cisco.com:
 Cisco Internetwork Operating System Software
IOS (tm) 3600 Software (C3640-A2IS-M), Experimental Version 12.2
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Wed 08-Aug-01 12:39 by joeuser
```

The following is sample output from the **show cdp entry protocol** command. Only information about the protocols enabled on *device.cisco.com* is displayed.

```
Router# show cdp entry device.cisco.com protocol

Protocol information for device.cisco.com:
  IP address: 10.1.17.24
  IPv6 address: FE80::203:E3FF:FE6A:BF81  (link-local)
  IPv6 address: 4000::BC:0:0:C0A8:BC06  (global unicast)
  CLNS address: 490001.1111.1111.1111.00
```

Related Commands

Command	Description
show cdp	Displays global CDP information, including timer and hold-time information.
show cdp interface	Displays information about the interfaces on which CDP is enabled.
show cdp neighbors	Displays detailed information about neighboring devices discovered using CDP.
show cdp traffic	Displays traffic information from the CDP table.

show cdp neighbors

To display detailed information about neighboring devices discovered using Cisco Discovery Protocol, use the **show cdp neighbors** command in privileged EXEC mode.

show cdp neighbors [*type number*] [**detail**]

Syntax Description

type	(Optional) Interface type that is connected to the neighbors about which you want information; possible valid values are **ethernet**, **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **port-channel**, and **vlan**.
number	(Optional) Number of the interface connected to the neighbors about which you want information.
detail	(Optional) Displays detailed information about a neighbor (or neighbors) including network address, enabled protocols, hold time, and software version.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
10.3	This command was introduced.
12.0(3)T	The output of this command using the **detail** keyword was expanded to include Cisco Discovery Protocol Version 2 information.
12.2(8)T	Support for IPv6 address and address type information was added.
12.2(14)S	Support for IPv6 address and address type information was added.
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(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 **vlan** keyword is supported in Cisco 7600 series routers that are configured with a Supervisor Engine 2.

The **port-channel** values are from 0 to 282; values from 257 to 282 are supported on the call switching module (CSM) and the firewall services module (FWSM) only.

Examples

The following is sample output from the **show cdp neighbors** command:

```
Router# show cdp neighbors

Capability Codes:R - Router, T - Trans Bridge, B - Source Route Bridge S - Switch,
```

```
H - Host, I - IGMP, r - Repeater
Device ID  Local Intrfce  Holdtme  Capability  Platform  Port ID
joe        Eth 0          133      R           4500      Eth 0
sam        Eth 0          152      R           AS5200    Eth 0
terri      Eth 0          144      R           3640      Eth0/0
maine      Eth 0          141                  RP1       Eth 0/0
sancho     Eth 0          164                  7206      Eth 1/0
```

Table 140 describes the fields shown in the display.

Table 141 show cdp neighbors Field Descriptions

Field	Definition
Capability Codes	The type of device that can be discovered.
Device ID	The name of the neighbor device and either the MAC address or the serial number of this device.
Local Intrfce	The local interface through which this neighbor is connected.
Holdtme	The remaining amount of time (in seconds) the current device will hold the Cisco Discovery Protocol advertisement from a sending router before discarding it.
Capability	The type of the device listed in the CDP Neighbors table. Possible values are as follows: • R—Router • T—Transparent bridge • B—Source-routing bridge • S—Switch • H—Host • I—IGMP device • r—Repeater
Platform	The product number of the device.
Port ID	The interface and port number of the neighboring device.

The following is sample output for one neighbor from the **show cdp neighbors detail** command. Additional detail is shown about neighbors, including network addresses, enabled protocols, and software version.

```
Router# show cdp neighbors detail

Device ID: device.cisco.com
Entry address(es):
  IPv6 address: FE80::203:E3FF:FE6A:BF81  (link-local)
  IPv6 address: 4000::BC:0:0:C0A8:BC06  (global unicast)
Platform: cisco 3640,  Capabilities: Router
Interface: Ethernet0/1,  Port ID (outgoing port): Ethernet0/1
Holdtime : 160 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) 3600 Software (C3640-A2IS-M), Version 12.2(25)SEB4, RELE)
advertisement version: 2
Duplex Mode: half
Native VLAN: 42
```

```
VTP Management Domain: 'Accounting Group'
```

Table 142 describes the fields shown in the display.

Table 142 show cdp neighbors detail Field Descriptions

Field	Definition
Device ID	The name of the neighbor device and either the MAC address or the serial number of this device.
Entry address(es)	A list of network addresses of neighbor devices.
IPv6 address: FE80::203:E3FF:FE6A:BF81 (link-local)	The network address of the neighbor device. The address can be in IP, IPv6, IPX, AppleTalk, DECnet, or Connectionless Network Service (CLNS) protocol conventions. IPv6 addresses are followed by one of the following IPv6 address types: • global unicast • link-local • multicast • site-local • V4 compatible **Note** For Cisco IOS Releases12.2(33)SXH3, Release 12.2(33)SXI and later releases, the command will not display the AppleTalk address.
Platform	The product name and number of the neighbor device.
Capabilities	The device type of the neighbor. This device can be a router, a bridge, a transparent bridge, a source-routing bridge, a switch, a host, an IGMP device, or a repeater.
Interface	The local interface through which this neighbor is connected.
Port ID	The interface and port number of the neighboring device.
Holdtime	The remaining amount of time (in seconds) the current device will hold the CDP advertisement from a sending router before discarding it.
Version	The software version of the neighbor device.
advertisement version:	Version of CDP that is being used for CDP advertisements.
Duplex Mode	The duplex state of connection between the current device and the neighbor device.
Native VLAN	The ID number of the VLAN on the neighbor device.
VTP Management Domain	A string that is the name of the collective group of VLANs associated with the neighbor device.

Related Commands

Command	Description
show cdp	Displays global CDP information, including timer and hold-time information.
show cdp entry	Displays information about a specific neighbor device listed in the CDP table.
show cdp interface	Displays information about the interfaces on which CDP is enabled.
show cdp traffic	Displays information about traffic between devices gathered using CDP.

show cef

To display information about packets forwarded by Cisco Express Forwarding, use the **show cef** command in privileged EXEC mode.

show cef {**accounting** | **background** [**detail**] | **broker** *broker-name* [**detail**] | **error** | **fib** | **hardware vectors** | **idb** | **loadinfo** | **non-ip** | **nsf** | **path** [**list** [**walk**] | **sets** [**detail** | **id** *path-set-id* | **summary**] | **switching background** [**detail**] | **walks** [**process** | **queue**]}

Syntax Description

accounting	Displays Cisco Express Forwarding accounting state.
background	Displays Cisco Express Forwarding background processing.
detail	(Optional) Displays detailed Cisco Express Forwarding information.
broker *broker-name*	(Distributed platforms only) Displays Cisco Express Forwarding information related to update brokers.
error	Displays information about the state of Cisco Express Forwarding errors.
fib	Displays Cisco Express Forwarding Forwarding Information Base (FIB) entries.
hardware vectors	Displays the hardware application programming interface (API) vector function table.
idb	Displays Cisco Express Forwarding interface descriptor blocks.
loadinfo	Displays Cisco Express Forwarding loadinfo events.
non-ip	Displays Cisco Express Forwarding paths for non-IP traffic.
nsf	(Distributed platforms only) Displays Cisco Express Forwarding nonstop forwarding (NSF) statistics.
path	Displays Cisco Express Forwarding paths.
list	(Optional) Displays a list of Cisco Express Forwarding paths.
walk	(Optional) Displays the walk through the list of Cisco Express Forwarding paths.
sets	(Optional) Displays point-to-multipoint path set information.
detail	(Optional) Displays detailed point-to-multipoint path set information.
id *path-set-id*	(Optional) Displays information about the specified path set. Enter the path set ID in hex format.
summary	(Optional) Displays high-level information about point-to-multipoint path sets.
switching background	Display Cisco Express Forwarding background switching processing.
walks	Specifies a walk through Cisco Express Forwarding infrastructure.
process	(Optional) Displays the process that services the background work queue.
queue	(Optional) Displays the work queue of background walks.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.2GS	This command was introduced to support the Cisco 12012 Internet router.
11.1CC	Support was added for multiple platforms.
12.0(22)S	The display output for this command was modified to include support for Cisco Express Forwarding for IPv6 and distributed Cisco Express Forwarding for IPv6 packets.
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(25)S	The **drop** and **not-cef-switched** keywords were removed. The **accounting**, **background**, **broker**, **fib**, **hardware vectors**, **idb**, **loadinfo**, **non-ip**, **nsf**, **path**, and **walks** 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.
12.2(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.
12.2(33)SRE	This command was modified. The **sets** keyword was added to display point-to-multipoint information.

Usage Guidelines

Use this command to display and monitor information about traffic forwarded by Cisco Express Forwarding.

A line card might drop packets because of encapsulation failure, absence of route information, or absence of adjacency information.

A packet is punted (sent to another switch path) because Cisco Express Forwarding may not support a specified encapsulation or feature, the packet may be destined for the router, or the packet may have IP options (such as time stamp and record route). IP options are process switched.

Examples

The following example shows how to display Cisco Express Forwarding accounting information:

```
Router# show cef accounting

IPv4 accounting state:
 Enabled accounting:            per-prefix, non-recursive, prefix-length
 Non-recursive load interval:   30 (default 30)
 Non-recursive update interval: 0 (default 0)

IPv6 accounting state:
 Enabled accounting:            None
 Non-recursive load interval:   30 (default 30)
 Non-recursive update interval: 0 (default 0)
```

Table 143 describes the significant fields shown in the example.

Table 143 show cef accounting Field Descriptions

Field	Description
Enabled accounting	Type or types of Cisco Express Forwarding accounting that are enabled: load-balance-hash, non-recursive, per-prefix, prefix-length, or none.
per-prefix	Indicates that Cisco Express Forwarding accounting is enabled for the collection of the number of packets and bytes express-forwarded to a destination (or prefix).
non-recursive	Indicates that Cisco Express Forwarding accounting is enabled through nonrecursive prefixes.
prefix-length	Indicates that Cisco Express Forwarding accounting is enabled through prefix length.

The following example shows how to display Cisco Express Forwarding background information:

```
Router# show cef background

CEF background process process (pid 77) running
 0 events awaiting registration on background process
 9 events registered on background process
  boolean   FIB malloc failed, 0 occurences
  boolean   FIB assert failed, 0 occurences
  boolean   FIB hw_api_failure failed, 0 occurences
  timer     FIB checkers: auto-repair delay, init, !run, 0 occurences
  timer     FIB checkers: auto-repair delay, init, !run, 0 occurences
  timer     FIB checkers: IPv4 scan-rib-ios scanner, init, run, 2 occurences
  timer     FIB checkers: IPv4 scan-ios-rib scanner, init, run, 2 occurences
  timer     FIB checkers: IPv6 scan-ios-rib scanner, init, run, 2 occurences
  timer     FIB table: rate monitor, init, run, 0 occurences
```

Table 144 describes the significant fields shown in the example.

Table 144 show cef background Field Descriptions

Field	Description
boolean	The background process is waiting for a true or false flag to be set.
FIB malloc failed, 0 occurences	No instances of memory allocation failure have occurred for the FIB.
FIB assert failed, 0 occurences	No instances of assertion failure have occurred for the FIB.
FIB hw_api_failure failed; 0 occurences	No failures are reported during the programming of hardware forwarding.
timer	The background process is waiting for a timer to be triggered. Once the timer is triggered, the operation begins. In the FIB checkers cases that follow, the timer is linked to Cisco Express Forwarding consistency checkers.
FIB checkers: auto-repair delay, init, !run, 0 occurences	FIB auto repair timer is initialized, but the timer is not running and has not been running (0 occurences).
FIB checkers: IPv4 scan-rib-ios scanner, init, !run, 2 occurences	FIB IPv4 scan-rib-ios timer is initialized and running. The timer has been triggered twice.

Table 144 show cef background Field Descriptions

Field	Description
FIB checkers: IPv4 scan-ios-rib scanner, init, run, 2 occurences	FIB IPv4 scan-ios-rib timer is initialized and running. The timer has been triggered twice.
FIB table: rate monitor, init, run, 0 occurences	FIB table rate monitor timer is initialized and running, but has yet to be triggered.

The following example shows how to display information about Cisco Express Forwarding FIB entries:

```
Router# show cef fib

9 allocated IPv4 entries, 0 failed allocations
1 allocated IPv6 entry, 0 failed allocations
```

Table 145 describes the significant fields shown in the example.

Table 145 show cef fib Field Descriptions

Field	Description
9 allocated IPv4 entries, 0 failed allocations	Number of successfully allocated and failed IPv4 entries.
1 allocated IPv6 entry, 0 failed allocations	Number of successfully allocated and failed IPv6 entries.

The following example shows how to display information about Cisco Express Forwarding loadinfo:

```
Router# show cef loadinfo

0 allocated loadinfos, 0 failed allocations
0 allocated loadinfo hash usage gsbs
0 inplace modifies (enabled)
0 identical modifies
```

Table 146 describes the significant fields shown in the example.

Table 146 show cef loadinfo Field Descriptions

Field	Description
0 allocated loadinfos, 0 failed allocations	Number of successfully allocated and failed allocated loadinfos.
0 allocated loadinfo hash usage gsbs	Number of allocated subblocks for per-hash bucket accounting when load balancing is used.
0 inplace modifies (enabled)	In-place modification is enabled. No in-place modifications have occurred.
0 identical modifies	Number of in-place modifications that were skipped because the replacement was identical to the target.

The following example shows how to display information for Cisco Express Forwarding paths:

```
Router# show cef path

28 allocated IPv4 paths, 0 failed allocations
4 allocated IPv6 paths, 0 failed allocations
```

```
32 Total Paths, 587 Recursive Paths, 0 Unresolved Paths
```

Table 147 describes the significant fields shown in the example.

Table 147 show cef path Field Descriptions

Field	Definition
28 allocated IPv4 paths	Number of successfully allocated and failed IPv4 paths.
4 allocated IPv6 paths	Number of successfully allocated and failed IPv4 paths.
32 Total Paths, 587 Recursive Paths, 0 Unresolved Paths	Information on all Cisco Express Forwarding paths.

The following example shows how to display information about Cisco Express Forwarding background switching processes:

```
Router# show cef switching background

CEF switching background process (pid 46) running
 0 events awaiting registration on background process
 1 event registered on background process
  boolean   OCE unlock queue, 0 occurences
```

Table 148 describes the significant fields shown in the example.

Table 148 show cef switching background Field Descriptions

Field	Description
0 events awaiting registration on background process	Number of events waiting to be registered on the background process.
1 event registered on background process	Number of events registered on the background process.
boolean OCE unlock queue, 0 occurences	Number of output chain element (OCE) unlock queue events.

The following example shows how to display information about Cisco Express Forwarding:

```
Router# show cef walks

Calling process:
----------------

Number of initial walks:

                        started
mode / priority             low          high     very high
sync                          3             0             0
atomic                        0             0             0

                       finished
mode / priority             low          high     very high
sync                          3             0             0
atomic                        0             0             0

                      restarted
mode / priority             low          high     very high
```

```
sync                          0             0             0
atomic                        0             0             0

Number of sub walks:

                         started
mode / priority              low          high     very high
sync                           0             0             0
atomic                         0             0             0

                        finished
mode / priority              low          high     very high
sync                           0             0             0
atomic                         0             0             0
```

Table 149 describes the significant fields shown in the example.

Table 149 show cef walks Field Description

Field	Description
mode	Indicates the mode of the Cisco Express Forwarding infrastructure walk: • sync—The walk takes place in the current process context and completes before the start function returns. Other processes are allowed to run. • atomic—The walk takes place in the current process context and completes before the start function returns. No other processes are allowed to run.
priority	Indicate the priority of the infrastructure walk: low, medium, or high.

Related Commands

Command	Description
clear cef linecard	Clears Cisco Express Forwarding information from line cards.
show cef features global	Displays Cisco Express Forwarding features for any interface.
show cef interface	Displays detailed Cisco Express Forwarding information for a specified interface or for all interfaces.
show cef linecard	Displays Cisco Express Forwarding-related information by line card.
show cef memory	Displays information about Cisco Express Forwarding memory usage.
show cef state	Displays the state of Cisco Express Forwarding on a networking device.
show cef subtree context client	Displays Cisco Express Forwarding prefix subtrees.
show cef table	Displays the configuration and operational state of the Cisco Express Forwarding FIB table.
show cef timers	Displays the current state of the timers internal to the Cisco Express Forwarding process.

show cef interface

To display detailed Cisco Express Forwarding information for a specified interface or for all interfaces, use the **show cef interface** command in user EXEC or privileged EXEC mode.

show cef interface [*type number*] [**statistics | detail | internal | brief | policy-statistics** [**input | output**]]

Syntax Description

type number	(Optional) Interface type and number. No space is required between the interface type and number.
statistics	(Optional) Displays switching statistics for an interface or interfaces.
detail	(Optional) Displays detailed Cisco Express Forwarding information for the specified interface type and number.
internal	(Optional) Displays internal Cisco Express Forwarding interface status and configuration.
brief	(Optional) Summarizes the Cisco Express Forwarding interface state.
policy-statistics	(Optional) Displays Border Gateway Protocol (BGP) policy statistical information for a specific interface or for all interfaces.
input	(Optional) Displays BGP accounting policy statistics for traffic that is traveling through an input interface.
output	(Optional) Displays BGP accounting policy statistics for traffic that is traveling through an output interface.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
11.2GS	This command was introduced to support the Cisco 12012 Internet router.
11.1CC	Support for multiple platforms was added.
12.0(14)ST	This command was integrated into Cisco IOS Release 12.0(14)ST, and the **statistics** keyword was added.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T, and the **detail** keyword was added.
12.2(13)T	The **policy-statistics** keyword was added.
12.0(22)S	The **input** and **output** keywords were added. The display output was modified to include support for Cisco Express Forwarding for IPv6 and distributed Cisco Express Forwarding interface information. Output fields that support BGP policy accounting were added for the Cisco 7200 series and Cisco 7500 series platforms.

Release	Modification
12.3(4)T	The **input** and **output** keywords were added. The display output was modified to include support for Cisco Express Forwarding for IPv6 and distributed Cisco Express Forwarding interface information. Output fields that support BGP policy accounting were added for the Cisco 7200 series and Cisco 7500 series platforms.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(25)S	The **internal** keyword was 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.
12.2(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

You can use this command to display the detailed Cisco Express Forwarding status for all interfaces.

Values entered for the *type* and *number* arguments display Cisco Express Forwarding status information for the specified interface type and number.

The **policy-statistics**, **input**, and **output** keywords are available only on distributed switching platforms.

Examples

The following example shows how to display a summary of Cisco Express Forwarding information for an interface named Ethernet 3/0:

```
Router# show cef interface ethernet 3/0 brief

Interface                      IP-Address      Status  Switching
Ethernet3/0                    10.0.212.6      up      CEF
Router#
```

The following is sample output from the **show cef interface** command for Fast Ethernet interface 1/0/0 with BGP policy accounting configured for input traffic:

```
Router# show cef interface fastethernet 1/0/0

FastEthernet1/0/0 is up (if_number 6)
  Corresponding hwidb fast_if_number 6
  Corresponding hwidb firstsw->if_number 6
  Internet address is 10.1.1.1/24
  ICMP redirects are always sent
  Per packet load-sharing is disabled
  IP unicast RPF check is disabled
  Inbound access list is not set
  Outbound access list is not set
  IP policy routing is disabled
  BGP based policy accounting on input is enabled
  BGP based policy accounting on output is disabled
Hardware idb is FastEthernet1/0/0 (6)
  Software idb is FastEthernet1/0/0 (6)
  Fast switching type 1, interface type 18
  IP Distributed CEF switching enabled
  IP Feature Fast switching turbo vector
  IP Feature CEF switching turbo vector
  Input fast flags 0x100, Output fast flags 0x0, Flags 0x0
```

```
  ifindex 7(7)
  Slot 1 Slot unit 0 VC -1
  Transmit limit accumulator 0xE8001A82 (0xE8001A82)
  IP MTU 1500
```

The following is sample output from the **show cef interface detail** command for Ethernet interface 1/0/0:

```
Router# show cef interface ethernet 1/0/0 detail

FastEthernet1/0/0 is up (if_number 6)
  Corresponding hwidb fast_if_number 6
  Corresponding hwidb firstsw->if_number 6
  Internet address is 10.1.1.1/24
  ICMP redirects are always sent
  Per packet load-sharing is disabled
  IP unicast RPF check is disabled
  Inbound access list is not set
  Outbound access list is not set
  IP policy routing is disabled
  BGP based policy accounting on input is enabled
  BGP based policy accounting on output is disabled
  Hardware idb is FastEthernet1/0/0 (6)
  Software idb is FastEthernet1/0/0 (6)
  Fast switching type 1, interface type 18
  IP Distributed CEF switching enabled
  IP Feature Fast switching turbo vector
  IP Feature CEF switching turbo vector
  Input fast flags 0x100, Output fast flags 0x0, Flags 0x0
  ifindex 7(7)
  Slot 1 Slot unit 0 VC -1
  Transmit limit accumulator 0xE8001A82 (0xE8001A82)
  IP MTU 1500
```

The following is sample output from the **show cef interface Null 0 detail** command:

```
Router# show cef interface null 0 detail

Null0 is up (if_number 1)
  Corresponding hwidb fast_if_number 1
  Corresponding hwidb firstsw->if_number 1
  Internet Protocol processing disabled
  Interface is marked as nullidb
  Packets switched to this interface on linecard are dropped to next slow path
  Hardware idb is Null0
  Fast switching type 13, interface type 0
  IP CEF switching enabled
  IP Feature CEF switching turbo vector
  Input fast flags 0x0, Output fast flags 0x0
  ifindex 0(0)
  Slot -1 Slot unit -1 VC -1
  Transmit limit accumulator 0x0 (0x0)
  IP MTU 1500
```

The following is sample output for internal Cisco Express Forwarding interface status and configuration for the Ethernet 3/1 interface:

```
Router# show cef interface ethernet 3/1 internal

Ethernet3/1 is up (if_number 13)
  Corresponding hwidb fast_if_number 13
  Corresponding hwidb firstsw->if_number 13
  Internet address is 10.0.212.6/24
  ICMP redirects are always sent
```

```
  Per packet load-sharing is disabled
  IP unicast RPF check is disabled
  Inbound access list is not set
  Outbound access list is not set
  IP policy routing is disabled
  BGP based policy accounting on input is disabled
  BGP based policy accounting on output is disabled
  Hardware idb is Ethernet3/1
  Fast switching type 1, interface type 63
  IP CEF switching enabled
  IP CEF switching turbo vector
  IP CEF turbo switching turbo vector
  IP prefix lookup IPv4 mtrie 8-8-8-8 optimized
  Input fast flags 0x0, Output fast flags 0x0
  ifindex 11(11)
  Slot 3 Slot unit 0 VC -1
  Transmit limit accumulator 0x0 (0x0)
  IP MTU 1500
 Subblocks:
  IPv6: enabled 1 unreachable FALSE redirect TRUE mtu 1500 flags 0x0
        link-local address is FE80::20C:CFFF:FEF9:4854
        Global unicast address(es):
        10:6:6:6:20C:CFFF:FEF9:4854, subnet is 10:6:6:6::/64 [EUI]
  IPv4: Internet address is 10.0.212.6/24
        Broadcast address 255.255.255.255
        Per packet load-sharing is disabled
        IP MTU 1500
```

Table 150 describes the significant fields shown in the displays.

Table 150 show cef interface Field Descriptions

Field	Description
FastEthernet1/0/0 is up	Indicates type, number, and status of the interface.
Internet address is	Internet address of the interface.
ICMP redirects are always sent	Indicates how packet forwarding is configured.
Per packet load-sharing is disabled	Indicates status of load sharing on the interface.
IP unicast RPF check is disabled	Indicates status of IP unicast Reverse Path Forwarding (RPF) check on the interface.
Inbound access list is not set	Indicates the number or name of the inbound access list if one is applied to this interface. Also indicates whether the list is set.
Outbound access list is not set	Indicates the number or name of the outbound access list if one is applied to this interface. Also indicates whether the list is set.
IP policy routing is disabled	Indicates the status of IP policy routing on the interface.
BGP based policy accounting on input is enabled	Indicates the status of BGP policy accounting on the input interface.
BGP based policy accounting on output is disabled	Indicates the status of BGP policy accounting on the output interface.
Hardware idb is Ethernet1/0/0	Interface type and number configured.

Table 150 show cef interface Field Descriptions (continued)

Field	Description
Fast switching type	Used for troubleshooting; indicates switching mode in use.
Interface type	Indicates interface type.
IP Distributed CEF switching enabled	Indicates whether distributed Cisco Express Forwarding is enabled on this interface. (Cisco 7500 and 12000 series Internet routers only.)
IP Feature Fast switching turbo vector	Indicates IP fast switching type configured.
IP Feature CEF switching turbo vector	Indicates IP feature Cisco Express Forwarding switching type configured.
Input fast flags	Indicates the input status of various switching features: • 0x0001 (input Access Control List [ACL] enabled) • 0x0002 (policy routing enabled) • 0x0004 (input rate limiting) • 0x0008 (MAC/Prec accounting) • 0x0010 (DSCP/PREC/QOS GROUP) • 0x0020 (input named access lists) • 0x0040 (NAT enabled on input) • 0x0080 (crypto map on input) • 0x0100 (QPPB classification) • 0x0200 (inspect on input) • 0x0400 (input classification) • 0x0800 ([1]casa input enable) • 0x1000 (Virtual Private Network [VPN] enabled on a [2]swidb) • 0x2000 (input idle timer enabled) • 0x4000 (unicast Reverse Path Forwarding [RPF] check) • 0x8000 (per-address ACL enabled) • 0x10000 (deaggregating a packet) • 0x20000 ([3]GPRS enabled on input) • 0x40000 (URL RenDezvous) • 0x80000 (QoS classification) • 0x100000 (FR switching on interface) • 0x200000 ([4]WCCP redirect on input) • 0x400000 (input classification)

Table 150 show cef interface Field Descriptions (continued)

Field	Description
Output fast flags	Indicates the output status of various switching features, as follows: • 0x0001 (output ACL enabled) • 0x0002 (IP accounting enabled) • 0x0004 (WCC redirect enabled interface) • 0x0008 (rate limiting) • 0x0010 (MAC/Prec accounting) • 0x0020 (DSCP/PREC/QOS GROUP) • 0x0040 (D-QOS classification) • 0x0080 (output named access lists) • 0x0100 (NAT enabled on output) • 0x0200 (TCP intercept enabled) • 0x0400 (crypto map set on output) • 0x0800 (output firewall) • 0x1000 ([5]RSVP classification) • 0x2000 (inspect on output) • 0x4000 (QoS classification) • 0x8000 (QoS preclassification) • 0x10000 (output stile)
ifindex 7/(7)	Indicates a Cisco IOS internal index or identifier for this interface.
Slot 1 Slot unit 0 VC -1	The slot number and slot unit.
Transmit limit accumulator	Indicates the maximum number of packets allowed in the transmit queue.
IP MTU	The MTU size set on the interface.

1. Cisco applications and services architecture (CASA)
2. Software interface descriptor block (SWIDB)
3. General packet radio system (GPRS)
4. Web cache communication protocol (WCCP)
5. Resource reservation protocol (RSVP)

The following is sample output from the **show cef interface command** using the **policy-statistics** keyword:

```
Router# show cef interface policy-statistics

POS7/0 is up (if_number 8)
Index   Packets                 Bytes

1           0                       0
2           0                       0
3           50                      5000
```

```
4          100                  10000
5          100                  10000
6          10                   1000
7          0                    0
8          0                    0
```

The following is sample output from the **show cef interface** command using the **policy-statistics** keyword. It shows policy statistics for Ethernet interface 1/0.

```
Router# show cef interface ethernet 1/0 policy-statistics

Ethernet1/0 is up (if_number 3)
  Corresponding hwidb fast_if_number 3
  Corresponding hwidb firstsw->if_number 3
 Index         Packets           Bytes
     1               0               0
     2               0               0
     3               0               0
     4               0               0
     5               0               0
     6               0               0
     7               0               0
     8               0               0
```

The following is sample output from the **show cef interface** command using the **policy-statistics** keyword. It shows policy statistics for Fast Ethernet interface 1/0/0 with the policy accounting based on input traffic.

```
Router# show cef interface fastethernet 1/0/0 policy-statistics input

FastEthernet1/0/0 is up (if_number 6)
  Corresponding hwidb fast_if_number 6
  Corresponding hwidb firstsw->if_number 6
  BGP based Policy accounting on input is enabled
 Index         Packets           Bytes
     1            9999          999900
     2               0               0
     3               0               0
     4               0               0
     5               0               0
     6               0               0
     7               0               0
     8               0               0
     9               0               0
    10               0               0
    11               0               0
    12               0               0
    13               0               0
    14               0               0
    15               0               0
    16               0               0
    17               0               0
    18               0               0
    19               0               0
    20               0               0
    21               0               0
    22               0               0
    23               0               0
    24               0               0
    25               0               0
    26               0               0
    27               0               0
    28               0               0
    29               0               0
```

```
    30              0               0
    31              0               0
    32              0               0
    33              0               0
    34           1234          123400
    35              0               0
    36              0               0
    37              0               0
    38              0               0
    39              0               0
    40              0               0
    41              0               0
    42              0               0
    43              0               0
    44              0               0
    45           1000          100000
    46              0               0
    47              0               0
    48              0               0
    49              0               0
    50              0               0
    51              0               0
    52              0               0
    53              0               0
    54           5123         1198782
```

The following is sample output from the **show cef interface** command using the **policy-statistics** keyword. It shows policy statistics for serial interface 1/1/2 with the policy accounting based on output traffic.

```
Router# show cef interface serial 1/1/2 policy-statistics output

Serial1/1/2 is up (if_number 9)
  Corresponding hwidb fast_if_number 9
  Corresponding hwidb firstsw->if_number 9
  BGP based Policy accounting on output is enabled
Index         Packets           Bytes
     1            9999          999900
     2               0               0
    .
    .
    .
    18              0               0
    19              0               0
    20              0               0
    .
    .
    .
    34           1234          123400
    35              0               0
    .
    .
    .
    44              0               0
    45           1000          100000
    46              0               0
    47              0               0
    48              0               0
    49              0               0
    50              0               0
    51              0               0
    52              0               0
    53              0               0
    54           5123         1198782
```

```
55                  0                   0
56                  0                   0
57                  0                   0
58                  0                   0
59                  0                   0
60                  0                   0
61                  0                   0
62                  0                   0
63                  0                   0
64                  0                   0
```

Table 151 describes the significant fields shown in the display.

Table 151 show cef interface policy-statistics Field Descriptions

Field	Description
Index	Traffic index set with the **route-map** command.
Packets	Number of packets switched that match the index definition.
Bytes	Number of bytes switched that match the index definition.

Related Commands

Command	Description
clear cef linecard	Clears Cisco Express Forwarding information from line cards.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol to another, or enables policy routing.
show cef	Displays information about packets forwarded by Cisco Express Forwarding.
show cef drop	Displays which packets the line cards dropped, or displays which packets were not express forwarded.
show cef linecard	Displays Cisco Express Forwarding interface information by line card.

show cef linecard

To display Cisco Express Forwarding-related information by line card, use the **show cef linecard** command in user EXEC or privileged EXEC mode.

show cef linecard [*slot-number*] [**detail**] [**internal**]

Syntax Description

slot-number	(Optional) Slot number for the line card about which to display Cisco Express Forwarding-related information. When you omit this argument, information about all line cards is displayed.
detail	(Optional) Displays detailed Cisco Express Forwarding information for the specified line card.
internal	(Optional) Displays internal Cisco Express Forwarding information for the specified line card.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
11.2 GS	This command was introduced to support the Cisco 12012 Internet router.
11.1 CC	Multiple platform support was added.
12.0(10)S	Output display was changed.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S, and the display output was modified to include support for Cisco Express Forwarding for IPv6 and distributed Cisco Express Forwarding for IPv6 line card information.
12.2(13)T	The display output modifications made in Cisco IOS Release 12.0(22)S were 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(25)S	The **events** keyword was removed.
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.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

This command is available only on distributed switching platforms.

When you omit the *slot-number* argument, information about all line cards is displayed. When you omit the *slot-number* argument and include the **detail** keyword, detailed information is displayed for all line cards. When you omit the *slot-number* argument and include the **internal** keyword, detailed internal information is displayed for all line cards.When you omit all keywords and arguments, the **show cef linecard** command displays important information about all line cards in table format.

Examples

The following is sample output from the **show cef linecard** command. The command displays information for all line cards in table format.

```
Router# show cef linecard

Slot    MsgSent    XDRSent  Window   LowQ   MedQ  HighQ Flags
0             6         95      24      0      0      0 up
1             6         95      24      0      0      0 up
VRF Default-table, version 8, 6 routes
Slot Version    CEF-XDR    I/Fs State    Flags
0          7          4       8 Active   up, sync
1          7          4      10 Active   up, sync
```

The following is sample output from the **show cef linecard detail** command for all line cards:

```
Router# show cef linecard detail

CEF linecard slot number 0, status up
 Sequence number 4, Maximum sequence number expected 28, Seq Epoch 2
 Send failed 0, Out Of Sequence 0, drops 0
 Linecard CEF reset 0, reloaded 1
 95 elements packed in 6 messages(3588 bytes) sent
 69 elements cleared
 linecard in sync after reloading
 0/0/0 xdr elements in LowQ/MediumQ/HighQ
 11/9/69 peak elements on LowQ/MediumQ/HighQ
 Input  packets 0, bytes 0
 Output packets 0, bytes 0, drops 0
 CEF Table statistics:
 Table name                Version Prefix-xdr Status
 Default-table                   7          4 Active, up, sync
CEF linecard slot number 1, status up
 Sequence number 4, Maximum sequence number expected 28, Seq Epoch 2
 Send failed 0, Out Of Sequence 0, drops 0
 Linecard CEF reset 0, reloaded 1
 95 elements packed in 6 messages(3588 bytes) sent
 69 elements cleared
 linecard in sync after reloading
 0/0/0 xdr elements in LowQ/MediumQ/HighQ
 11/9/69 peak elements on LowQ/MediumQ/HighQ
 Input  packets 0, bytes 0
 Output packets 0, bytes 0, drops 0
 CEF Table statistics:
 Table name                Version Prefix-xdr Status
 Default-table                   7          4 Active, up, sync
```

The following is sample output from the **show cef linecard internal** command for all line cards:

```
Router# show cef linecard internal

CEF linecard slot number 0, status up
 Sequence number 11, Maximum sequence number expected 35
 Send failed 0, Out Of Sequence 0
 Linecard CEF reset 2, reloaded 2
 Total elements queued:
  prefix                   4
  adjacency                4
  interface                91
  address                  2
  policy routing           2
  hw interface             57
  state                    6
  resequence               2
  control                  13
```

```
 table                    2
 time                     4484
 flow features deactivate 2
 flow cache config        2
 flow export config       2
 dss                      2
 isl                      2
 mpls atm vc remove       2
 mpls atm vc set label    2
                          2
                          2
                          3
                          1
4574 elements packed in 4495 messages(90286 bytes) sent
115 elements cleared
Total elements cleared:
 prefix                   2
 adjacency                1
 interface                63
 address                  1
 policy routing           1
 hw interface             29
 state                    2
 control                  5
 table                    1
 flow features deactivate 1
 flow cache config        1
 flow export config       1
 dss                      1
 isl                      1
 mpls atm vc remove       1
 mpls atm vc set label    1
                          1
                          1
                          1
linecard disabled  - failed a reload
0/0/0 xdr elements in LowQ/MediumQ/HighQ
Input  packets 0, bytes 0
Output packets 0, bytes 0, drops 0

CEF Table statistics:
Table name               Version Prefix-xdr Status
Default-table                  8          4 Active, sync
```

Table 152 describes the significant fields shown in the displays.

Table 152 show cef linecard Field Descriptions

Field	Description
Table name	Name of the Cisco Express Forwarding table.
Version	Number of the Forwarding Information Base (FIB) table version.
Prefix-xdr	Number of prefix IPC information elements external data representation (XDRs) processed.
Status	State of the Cisco Express Forwarding table.
Slot	Slot number of the line card.
MsgSent	Number of interprocess communications (IPC) messages sent.
XDRSent	XDRs packed into IPC messages sent from the Route Processor (RP) to the line card.

Table 152 show cef linecard Field Descriptions (continued)

Field	Description
Window	Size of the IPC window between the line card and the RP.
LowQ/MedQ/HighQ	Number of XDR elements in the Low, Medium, and High priority queues.
Flags	Indicates the status of the line card. States are: • up—Line card is up. • sync—Line card is in synchronization with the main FIB. • FIB is repopulated on the line card. • reset—Line card FIB is reset. • reloading—Line card FIB is being reloaded. • disabled—Line card is disabled.
CEF-XDR	Number of Cisco Express Forwarding XDR messages processed.
I/Fs	Interface numbers.

Related Commands

Command	Description
show cef	Displays which packets the line cards dropped or displays which packets were not express-forwarded.
show cef interface	Displays Cisco Express Forwarding-related interface information.
show ipv6 cef	Displays entries in the IPv6 FIB.

show cef table

To display the configuration and operational state of the Cisco Express Forwarding Forwarding Information Base (FIB) table, use the **show cef table** command in privileged EXEC mode.

Cisco IOS 12.2(33)SRB and Later S-Based Releases

show cef table [**consistency-check** | **detail** | **internal** | [**ipv4** | **ipv6**] [**vrf** {***** | **Default** | *vrf-name*}] [**topology** {***** | **base** | *topology-name*}] [**detail** | **internal**]]

Cisco IOS 12.4(20)T and Later T-Based Releases

show cef table [**consistency-check** | **detail** | **internal** | [**ipv4** | **ipv6**] {**Default** | *vrf-name*} [**detail** | **internal**]]

Syntax Description

consistency-check	(Optional) Displays the status of consistency checkers in the FIB.
detail	(Optional) Displays detailed Cisco Express Forwarding operational status and configuration.
internal	(Optional) Displays internal Cisco Express Forwarding operational status and configuration.
ipv4	(Optional) Displays operational status for IPv4 from the IPv4 FIB.
ipv6	(Optional) Displays operational status for IPv6 from the IPv6 FIB.
vrf	(Optional) Specifies a Virtual Private Network (VPN) routing and forwarding (VRF) instance for the specified address family.
*****	Displays operational status for all configured VRFs (**vrf ***) or all topologies (**topology ***), respectively.
Default	Displays operational status for the default VRF for the specified address family.
vrf-name	Displays operational status for the named VRF configured for the specified address family.
topology	(Optional) Specifies a topology for the selected address family.
base	Displays operational status for the base topology for the specified address family.
topology-name	Displays operational status for the identified topology-specific table.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 2.2(28)SB.
12.2(33)SRA	This command was introduced.
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 display information about the configuration and operational statistics for Cisco Express Forwarding IPv4 FIB and IPv6 FIB.

Cisco IOS 12.4(20)T and Later T-based Releases

When you enter an **ipv4** or **ipv6** keyword with the **show cef table** command, you must enter the name of a configured VRF or the **Default** keyword.

Cisco IOS 12.2(33)SRB and Later S-based Releases

The **vrf** and **topology** keywords are optional when you enter the **ipv4** or **ipv6** keyword with the **show cef table** command.

Examples

The following is sample output from the **show cef table** command:

```
Router# show cef table

Global information:
 Output chain build favors:
  platform:      not configured
  CLI:           not configured
  operational:   convergence-speed
 Output chain build characteristics:
  Inplace modify
     operational for:     load-sharing
 Collapse
     operational for:     load-sharing
 Indirection
     operational for:     recursive-prefix
 MTRIE information:
  TAL: node pools:
   pool[C/8 bits]: 12 allocated (0 failed), 12480 bytes {1 refcount}


1 active IPv4 table (9 prefixes total) out of a maximum of 10000.
VRF                      Prefixes       Memory  Flags
Default                         9        13520

1 active IPv6 table (1 prefix total) out of a maximum of 10000.
VRF                      Prefixes       Memory  Flags
VRF                      Prefixes       Memory  Flags
Default                         1          208
```

Table 153 describes significant fields shown in the display.

Table 153 show cef table Field Descriptions

Field	Description
Output chain build favors:	Indicates table output chain building operational preferences.
Platform: not configured	Output chain building characteristics are not explicitly set or supported by the platform. The default output chain building characteristics are used.
CLI: not configured	Output chain building characteristics are not explicitly configured. The default is used.
operational: convergence speed	Output chain building favors convergence. This is the default operational behavior.

Table 153 show cef table Field Descriptions (continued)

Field	Description
Output chain build characteristics	Indicates the output chain building characteristics.
Inplace modify operational for: load-sharing	Indicates that the load sharing information in effect can be changed if the output information of the Interior Gateway Protocol (IGP) changes.
Collapse operational for: load-sharing	Indicates that the load-sharing tree is collapsed if load balancing is not affected.
Indirection operational for: recursive-prefix	Indicates that the use of indirection objects is enabled for recursive prefixes.
MTRIE information:	Indicates that information about the multi-array retrieval (MTRIE) follows.
TAL: node pools:	Indicates that node pool information for the Tree Abstraction Layer (TAL) follows.
pool (C/8 bits):	Indicates the memory management technique for the pool and the stride size (8 bits). The C indicates the use of a chunk pool. An M would indicate the use of a malloc.

The following is sample output from the **show cef table internal** command:

```
Router# show cef table internal

Table: IPv4:Default (id 0)
 sources:               Default table
 ref count:             31
 flags (0x00):          none
 smp allowed:           yes
 default network:       none
 route count:           9
 route count (fwd):     9
 route count (non-fwd): 0
 Database epoch:        0 (9 entries at this epoch)
 Subblocks:

  These rates are ndbs/minute.
   RIB update rate:           0
   RIB update peak rate:      0
 Internals:
  table:            0x4BFA060
  extra:            0x000000
  broker record:    0x000000
  tal root:         0x4C01988
  lookup OCE:       0x4C12B50


Table: IPv6:Default (id 0)
 sources:               Default table
 ref count:             3
 flags (0x00):          none
 smp allowed:           no
 default network:       none
 route count:           1
 route count (fwd):     1
 route count (non-fwd): 0
 Database epoch:        0 (1 entry at this epoch)
```

```
 Subblocks:

  These rates are ndbs/minute.
   RIB update rate:           0
   RIB update peak rate:      0
Internals:
 table:            0x4BF9FF0
 extra:            0x000000
 broker record:    0x000000
 tal root:         0x4C96328
 lookup OCE:       0x4C12B30
```

Table 154 describes significant fields shown in the display.

Table 154 show cef table internal Field Descriptions

Field	Description
Table: IPv4: Default (id 0)	The FIB table, IPv4 or IPv6, for which operation statistics follow.
sources: Default table	The source of the information comes from the Default table.
ref count: 3	The number of internal pointers to the VRF table structure.
flags (0x00): none	No flags are configured.
smp allowed: yes	Symmetrical Multi-Processing (SMP) is allowed.
default network: none	A default network is not configured.
route count: 9	Total number of routes is 9.
route count (fwd): 9	The number of routes forwarded is 9.
route count (non-fwd): 0	The number of routes not forwarded is 0.
Database epoch: 0 (9 entries at this epoch)	Epoch number (table version) is 0 and contains 9 entries.
Subblocks:	No subblocks are defined.
RIB update rate: 0	No update rate is configured for the RIB.
RIB update peak rate 0	No peak update rate is defined for the RIB.
Internal:	Identification for Cisco Express Forwarding internal operations.

The following is sample output from the **show cef table consistency-check** command:

```
Router# show cef table consistency-check

Consistency checker master control: enabled

IPv4:
 Table consistency checker state:
  scan-rib-ios: disabled
   0/0/0/0 queries sent/ignored/checked/iterated
  scan-ios-rib: disabled
   0/0/0/0 queries sent/ignored/checked/iterated
  full-scan-rib-ios: enabled [1000 prefixes checked every 60s]
   0/0/0/0 queries sent/ignored/checked/iterated
  full-scan-ios-rib: enabled [1000 prefixes checked every 60s]
   0/0/0/0 queries sent/ignored/checked/iterated
 Checksum data checking disabled
```

```
 Inconsistency error messages are disabled
 Inconsistency auto-repair is enabled (10s delay, 300s holddown)
 Inconsistency auto-repair runs: 0
 Inconsistency statistics: 0 confirmed, 0/16 recorded

IPv6:
 Table consistency checker state:
  scan-ios-rib: disabled
   0/0/0/0 queries sent/ignored/checked/iterated
  full-scan-rib-ios: enabled [1000 prefixes checked every 60s]
   0/0/0/0 queries sent/ignored/checked/iterated
  full-scan-ios-rib: enabled [1000 prefixes checked every 60s]
   0/0/0/0 queries sent/ignored/checked/iterated
 Checksum data checking disabled
 Inconsistency error messages are disabled
 Inconsistency auto-repair is enabled (10s delay, 300s holddown)
 Inconsistency auto-repair runs: 0
 Inconsistency statistics: 0 confirmed, 0/16 recorded
```

Table 155 describes significant fields shown in the display.

Table 155 show cef table consistency-check Field Descriptions

Field	Description
scan-rib-ios: disabled	The consistency checker that compares the Routing Information Base (RIB) to the FIB table and provides the number of entries missing from the FIB table is disabled.
scan-ios-rib: disabled	The consistency checker that compares the FIB table to the RIB and provides the number of entries missing from the RIB is disabled.
full-scan-rib-ios: enabled	A full scan is enabled that compares the RIB to the FIB table. Every 60 seconds, 1000 prefixes are checked.
full-scan-ios-rib: enabled	A full scan is enabled that compares the FIB table to the RIB. Every 60 seconds, 1000 prefixes are checked.
Checksum data checking disabled	The data-checking function is disabled.
Inconsistency error messages are disabled	The consistency checker to generate inconsistency error messages is disabled.
Inconsistency auto-repair is enabled (10s delay, 300s holddown)	The auto repair function is enabled with the default settings of a 10-second delay and a 300-second holddown.

The following is sample output from the **show cef table IPv4 Default** command:

```
Router# show cef table ipv4 Default

Table: IPv4:Default (id 0)
 sources:               Default table
 ref count:             31
 flags (0x00):          none
 smp allowed:           yes
 default network:       none
 route count:           9
 route count (fwd):     9
 route count (non-fwd): 0
 Database epoch:        0 (9 entries at this epoch)
 Subblocks:
```

```
  These rates are ndbs/minute.
   RIB update rate:           0
   RIB update peak rate:      0
```

For a description of significant fields shown in the display, see Table 154.

The following is sample output from the **show cef table IPv6 Default internal** command:

```
Router# show cef table ipv6 Default internal

Table: IPv6:Default (id 0)
 sources:               Default table
 ref count:             3
 flags (0x00):          none
 smp allowed:           no
 default network:       none
 route count:           1
 route count (fwd):     1
 route count (non-fwd): 0
 Database epoch:        0 (1 entry at this epoch)
 Subblocks:

  These rates are ndbs/minute.
   RIB update rate:           0
   RIB update peak rate:      0
 Internals:
  table:            0x4BF9FF0
  extra:            0x000000
  broker record:    0x000000
  tal root:         0x4C96328
  lookup OCE:       0x4C12B30
```

For a description of significant fields shown in the display, see Table 154.

Related Commands

Command	Description
cef table consistency-check	Enables Cisco Express Forwarding table consistency checker types and parameters.
cef table output-chain build	Configures Cisco Express Forwarding table output chain building characteristics for the forwarding of packet through the network.
show cef	Displays information about packets forwarded by Cisco Express Forwarding.

show clns neighbors

To display end system (ES), intermediate system (IS), and multitopology Integrated Intermediate System-to-Intermediate System (M-ISIS) neighbors, use the **show clns neighbors** command in user EXEC or privileged EXEC mode.

show clns neighbors [*process-tag*] [*interface-type interface-number*] [**area**] [**detail**]

Syntax Description

process-tag	(Optional) A unique name among all International Organization for Standardization (ISO) router processes including IP and Connectionless Network Service (CLNS) router processes for a given router. If a process tag is specified, output is limited to the specified routing process. When **null** is specified for the process tag, output is displayed only for the router process that has no tag specified. If a process tag is not specified, output is displayed for all processes.
interface-type	(Optional) Interface type.
interface-number	(Optional) Interface number.
area	(Optional) Displays the CLNS multiarea adjacencies.
detail	(Optional) Displays the area addresses advertised by the neighbor in the hello messages. Otherwise, a summary display is provided. In IPv6, this keyword displays the address family of the adjacency.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.0(5)T	The **area** and **detail** keywords were added.
12.2(15)T	Support was added for IPv6.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.0(29)S	The *process-tag* argument was 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.
12.2(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 2.4	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The **show clns neighbors** command displays the adjacency that is learned through multitopology IS-IS for IPv6.

Examples

The following is sample output from the **show clns neighbors** command:

```
Router# show clns neighbors

System Id          Interface    SNPA            State  Holdtime  Type Protocol
0000.0000.0007     Et3/3        aa00.0400.6408  UP     26        L1   IS-IS
0000.0C00.0C35     Et3/2        0000.0c00.0c36  Up     91        L1   IS-IS
0800.2B16.24EA     Et3/3        aa00.0400.2d05  Up     27        L1   M-ISIS
0800.2B14.060E     Et3/2        aa00.0400.9205  Up     8         L1   IS-IS
```

The following is sample output from the **show clns neighbors** command using the *process-tag* argument to display information about the VRF-aware IS-IS instance tag1:

```
Router# show clns tagRED neighbors

Tag tag1:
System Id          Interface    SNPA            State  Holdtime  Type Protocol
igp-03             Fa0/         200d0.2b7f.9502 Up     9         L2   IS-IS
igp-03             PO2/2.1      DLCI 211        Up     27        L2   IS-IS
igp-02             PO2/0.1      DLCI 131        Up     29        L2   IS-IS
igp-11             Fa0/4        000e.d79d.7920  Up     7         L2   IS-IS
igp-11             Fa0/5        000e.d79d.7921  Up     8         L2   IS-IS
igp-11             PO3/2.1      DLCI 451        Up     24        L2   IS-IS
```

The following is sample output from the **show clns neighbors** command using the **detail** keyword:

```
Router# show clns neighbors detail

System Id          Interface    SNPA            State  Holdtime  Type Protocol
0000.0000.0007     Et3/3        aa00.0400.6408  UP     26        L1   IS-IS

Area Address(es): 20
IP Address(es): 172.16.0.42*
Uptime: 00:21:49
0000.0C00.0C35     Et3/2        0000.0c00.0c36  Up     91        L1   IS-IS

Area Address(es): 20
IP Address(es): 192.168.0.42*
Uptime: 00:21:52
0800.2B16.24EA     Et3/3        aa00.0400.2d05  Up     27        L1   M-ISIS

Area Address(es): 20
IP Address(es): 192.168.0.42*
IPv6 Address(es): FE80::2B0:8EFF:FE31:EC57
Uptime: 00:00:27
Topology: IPv6
0800.2B14.060E     Et3/2        aa00.0400.9205  Up     8         L1   IS-IS

Area Address(es): 20
IP Address(es): 192.168.0.30*
Uptime: 00:21:52
```

The following is sample output from the **show clns neighbors** command using the *process-tag* argument to display information about the VRF-aware IS-IS instance tagSecond:

```
Router# show clns tagSecond neighbors

Tag tagSecond:

System Id      Interface   SNPA            State  Holdtime  Type Protocol
igp-03         Fa0/2       00d0.2b7f.9502  Up     9         L2   IS-IS
igp-03         PO2/2.1     DLCI 211        Up     27        L2   IS-IS
igp-02         PO2/0.1     DLCI 131        Up     29        L2   IS-IS
igp-11         Fa0/4       000e.d79d.7920  Up     7         L2   IS-IS
```

```
igp-11          Fa0/5        000e.d79d.7921      Up     8          L2   IS-IS
igp-11          PO3/2.1      DLCI 451            Up     24         L2   IS-IS
```

Table 156 describes the significant fields shown in the display.

Table 156 show clns neighbors Field Descriptions

Field	Description
Tag tagSecond	Tag name that identifies an IS-IS instance.
System Id	Six-byte value that identifies a system in an area.
Interface	Interface from which the system was learned.
SNPA	Subnetwork Point of Attachment. This is the data-link address.
State	State of the ES, IS, or M-ISIS.
Init	System is an IS and is waiting for an IS-IS hello message. IS-IS regards the neighbor as not adjacent.
Up	Believes the ES or IS is reachable.
Holdtime	Number of seconds before this adjacency entry times out.
Type	The adjacency type. Possible values are as follows: • ES—End-system adjacency either discovered via the ES-IS protocol or statically configured. • IS—Router adjacency either discovered via the ES-IS protocol or statically configured. • M-ISIS—Router adjacency discovered via the multitopology IS-IS protocol. • L1—Router adjacency for Level 1 routing only. • L1L2—Router adjacency for Level 1 and Level 2 routing. • L2—Router adjacency for Level 2 only.
Protocol	Protocol through which the adjacency was learned. Valid protocol sources are ES-IS, IS-IS, ISO IGRP, Static, DECnet, and M-ISIS.

Notice that the information displayed in the **show clns neighbors detail** command output includes everything shown in **show clns neighbors** command output in addition to the area address associated with the IS neighbor and its uptime. When IP routing is enabled, Integrated-ISIS adds information to the output of the **show clns** commands. The **show clns neighbors detail** command output shows the IP addresses that are defined for the directly connected interface and an asterisk (*) to indicate which IP address is the next hop.

show clock

To display the time and date from the system software clock, use the **show clock** command in user EXEC or privileged EXEC mode.

show clock [**detail**]

Syntax Description

detail	(Optional) Indicates the clock source (NTP, VINES, hardware clock, and so on) and the current summer-time setting (if any).

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(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.

Usage Guidelines

The software clock keeps an "authoritative" flag that indicates whether the time is authoritative (believed to be accurate). If the software clock has been set by a timing source (for example, via NTP), the flag is set. If the time is not authoritative, it will be used only for display purposes. Until the clock is authoritative and the "authoritative" flag is set, the flag prevents peers from synchronizing to the software clock.

The symbol that precedes the **show clock** display indicates the following:

Symbol	Description	Example
*	Time is not authoritative: the software clock is not in sync or has never been set.	*15:29:03.158 UTC Tue Feb 25 2003:
(blank)	Time is authoritative: the software clock is in sync or has just been set manually	15:29:03.158 UTC Tue Feb 25 2003:
.	Time is authoritative, but NTP is not synchronized: the software clock was in sync, but has since lost contact with all configured NTP servers	.15:29:03.158 UTC Tue Feb 25 2003:

These symbols are also used in NTP-based timestamping, such as for syslog (SEM) messages.

Note In general, NTP synchronization takes approximately 15 to 20 minutes.

Examples

The following sample output shows that the current clock is authoritative and that the time source is NTP:

```
Router> show clock detail

15:29:03.158 PST Tue Feb 25 2003
Time source is NTP
```

The following example shows the current clock is authoritative, but NTP is not yet synchronized:

```
Router> show clock

.16:42:35.597 UTC Tue Feb 25 2003
```

Related Commands

Command	Description
clock set	Manually sets the software clock.
show calendar	Displays the current time and date setting of the system hardware clock.

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 157 describes the significant fields shown in the display.

Table 157 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 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 158 describes the significant fields shown in the display.

Table 158 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 158 describes the significant fields shown in the display.

Table 159 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 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** [*ipv4-address* | *ipv6-address*] | **remote** [*ipv4-address* | *ipv6-address*] | **fvrf** *vrf-name*} [**detailed**]

Syntax Description

local [*ipv4-address* | *ipv6-address*]	Displays the current IKEv2 security associations matching the local IP address.
remote [*ipv4-address* | *ipv6-address*]	Displays the current IKEv2 security associations matching the remote IP 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.
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 current IKEv2 security associations.

Examples

The following are sample outputs 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

Router# show crypto ikev2 sa

Tunnel-id   Local          Remote           fvrf/ivrf          Status
1       2001:DB8:0::1/500    2001:DB8:0::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
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: 86400/479 sec
      CE id: 0, Session-id: 2, MIB-id: 2
      Status Description: Negotiation done
      Local spi: BCF1453548BE731C       Remote spi: 85CB158F05817B3A
      Local id:          10.0.0.1     Remote id:          10.0.0.2
      Local req mess id:    3           Remote req mess id: 0
      Local next mess id:    3          Remote next mess id: 1
      Local req queued:    3            Remote req queued: 0
      Local window:    5                 Remote window: 5
      DPD configured for 0 seconds
      NAT-T is not detected
```

Table 160 describes the significant fields shown in the display.

Table 160 show crypto ikev2 sa detailed Field Descriptions

Field	Description
Tunnel-id	Unique identifier of the IKEv2 tunnel.
Local	IP address (IPv4 or IPv6) and UDP port of the local IKEv2 endpoint.
Remote	IP address (IPv4 or IPv6) 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.

Table 160 show crypto ikev2 sa detailed Field Descriptions (continued)

Field	Description
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.
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 160 describes the significant fields shown in the display.

Table 161 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 161 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 ipsec policy

To display the parameters for each IP Security (IPsec) policy, use the **show crypto ipsec policy** command in user EXEC or privileged EXEC mode.

show crypto ipsec policy [**name** *policy-name*]

Syntax Description

name *policy-name*	(Optional) The specific policy for which parameters will be displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.4(4)T	Support for IPv6 was added.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

If no policy is specified, then information about all policies is displayed.

Examples

The following is sample output from the **show crypto ipsec policy** command:

```
Router# show crypto ipsec policy

Crypto IPsec client security policy data

Policy name:     OSPFv3-1-1000
Policy refcount: 1
Inbound  AH SPI: 1000 (0x3E8)
Outbound AH SPI: 1000 (0x3E8)
Inbound  AH Key: 1234567890ABCDEF1234567890ABCDEF
Outbound AH Key: 1234567890ABCDEF1234567890ABCDEF
Transform set:   ah-md5-hmac
```

Table 162 describes the significant fields shown in the display.

Table 162 show crypto ipsec policy Field Descriptions

Field	Description
Policy name	Specifies the name of the policy.
Inbound AH SPI	The authentication header (AH) security policy index (SPI) for inbound links.
Outbound AH SPI	The AH SPI for outbound links.
Inbound AH Key	The AH key for inbound links.

Table 162 show crypto ipsec policy Field Descriptions (continued)

Field	Description
Outbound AH Key	The AH key for outbound links.
Transform set	The transform set, which is an acceptable combination of security protocols and algorithms.

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 163 describes the significant fields shown in the above displays (**show crypto ipsec sa** and **show crypto ipsec sa detail**).

Table 163 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 163 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 163 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 164 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 164.

Table 164 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 165 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 165 or Table 164.

Table 165 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 163, Table 164, or Table 165.

```
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 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 166 describes significant fields in the **show crypto isakmp key** profile.

Table 166 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 65 describes the significant fields shown in the display.

Table 65 show crypto isakmp profile Field Descriptions

Field	Description
ISAKMP PROFILE	Name of the ISAKMP profile.

Table 65 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 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 66 describes the significant fields shown in the display.

Table 66 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 66 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 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** *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 of 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 67 describes the significant fields shown in the display.

Table 67 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 68 for explanations of the status of the IKE SA, IPsec SA, and tunnel as shown in the display.
IKE SA	Information is provided 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 map, number of encrypted or decrypted packets or dropped packets, and the IPsec SA remaining lifetime in kilobytes per second.

Table 68 provides an explanation of the current status of the VPN sessions shown in the display.

Table 68 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 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.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

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 its 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"
```

Significant fields are described in Table 69.

Table 69 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.
Crypto Sockets in Listen state	Name of the crypto IPSec profile.
Flags	If this field says “shared,” the socket is shared with more than one tunnel interface.

show dial-peer voice

To display information for voice dial peers, use the **show dial-peer voice** command in user EXEC or privileged EXEC mode.

show dial-peer voice [*number* | **busy-trigger-counter** | **summary** | **voip system**]

Syntax Description

number	(Optional) A specific voice dial peer. The output displays detailed information about that dial peer.
busy-trigger-counter	(Optional) Displays the busy trigger call count on the VoIP dial peer.
summary	(Optional) Displays a short summary of each voice dial peer.
voip system	(Optional) Displays information about the VoIP dial peer.

Command Default

If both the *number* argument and **summary** keyword are omitted, the output displays detailed information about all voice dial peers.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
11.3(1)T	This command was introduced.
11.3(1)MA	This command was modified. The **summary** keyword was added for the Cisco MC3810.
12.0(3)XG	This command was implemented for Voice over Frame Relay (VoFR) on the Cisco 2600 series and Cisco 3600 series.
12.0(4)T	This command was implemented for VoFR on the Cisco 7200 series.
12.1(3)T	This command was implemented for modem pass-through over VoIP on the Cisco AS5300.
12.2(2)XB	This command was modified to support VoiceXML applications.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.
12.2(2)XN	This command was modified. Support for enhanced Media Gateway Control Protocol (MGCP) voice gateway interoperability was added to Cisco CallManager 3.1 for the Cisco 2600 series, Cisco 3600 series, and Cisco VG200.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and Cisco CallManager 3.2 and implemented on the Cisco IAD2420. The command was enhanced to display configuration information for bandwidth, video codec, and rtp payload-type for H.263+ and H.264 video codec.

Release	Modification
12.4(22)T	This command was modified. This command was enhanced to display the current configuration state of the history-info header. Command output was updated to show IPv6 information.
15.0(1)XA	This command was modified. The output was enhanced to show the logical partitioning class of restriction (LPCOR) policy for outgoing calls.
15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.
15.1(3)T	This command was modified. The output was enhanced to display information about the bind at the dial-peer level and to display the connection status of Foreign Exchange Office (FXO) ports.

Usage Guidelines

Use this command to display the configuration for all VoIP and POTS dial peers configured for a gateway. To display configuration information for only one specific dial peer, use the *number* argument. To display summary information for all dial peers, use the **summary** keyword.

Examples

The following is sample output from the **show dial-peer voice** command for a POTS dial peer:

```
Router# show dial-peer voice 100

VoiceEncapPeer3201
peer type = voice, information type = video,
description = `',
tag = 3201, destination-pattern = `86001',
answer-address = `', preference=0,
CLID Restriction = None
CLID Network Number = `'
CLID Second Number sent
CLID Override RDNIS = disabled,
source carrier-id = `',target carrier-id = `',
source trunk-group-label = `',target trunk-group-label = `',
numbering Type = `unknown'
group = 3201, Admin state is up, Operation state is up,
Outbound state is up,
incoming called-number = `', connections/maximum = 0/unlimited,
DTMF Relay = disabled,
URI classes:
        Destination =
huntstop = disabled,
in bound application associated: 'DEFAULT'
out bound application associated: ''
dnis-map =
permission :both
        incoming COR list:maximum capability
outgoing COR list:minimum requirement
Translation profile (Incoming):
Translation profile (Outgoing):
incoming call blocking:
translation-profile = `'
disconnect-cause = `no-service'
advertise 0x40 capacity_update_timer 25 addrFamily 4 oldAddrFamily 4
type = pots, prefix = `',
forward-digits 4
session-target = `', voice-port = `2/0:23',
direct-inward-dial = enabled,
digit_strip = enabled,
```

```
register E.164 number with H323 GK and/or SIP Registrar = TRUE
fax rate = system,   payload size =  20 bytes
supported-language = ''
preemption level = `routine'
bandwidth:
        maximum = 384 KBits/sec, minimum = 64 KBits/sec
voice class called-number:
        inbound = `', outbound = `1'
Time elapsed since last clearing of voice call statistics never
        Connect Time = 0, Charged Units = 0,
Successful Calls = 0, Failed Calls = 0, Incomplete Calls = 0
Accepted Calls = 0, Refused Calls = 0,
Last Disconnect Cause is "",
Last Disconnect Text is "",
Last Setup Time = 0.
```

The following is sample output from this command for a VoIP dial peer:

```
Router# show dial-peer voice 101

VoiceOverIpPeer101
peer type = voice, system default peer = FALSE, information type = voice,
description = `',
tag = 1234, destination-pattern = `',
voice reg type = 0, corresponding tag = 0,
allow watch = FALSE
answer-address = `', preference=0,
CLID Restriction = None
CLID Network Number = `'
CLID Second Number sent
CLID Override RDNIS = disabled,
rtp-ssrc mux = system
source carrier-id = `', target carrier-id = `',
source trunk-group-label = `',  target trunk-group-label = `',
numbering Type = `unknown'
group = 1234, Admin state is up, Operation state is down,
incoming called-number = `', connections/maximum = 0/unlimited,
DTMF Relay = disabled,
modem transport = system,
URI classes:
Incoming (Request) =
Incoming (Via) =
Incoming (To) =
Incoming (From) =
Destination =
huntstop = disabled,
in bound application associated: 'DEFAULT'
out bound application associated: ''
dnis-map =
permission :both
incoming COR list:maximum capability
outgoing COR list:minimum requirement
outgoing LPCOR:
Translation profile (Incoming):
Translation profile (Outgoing):
incoming call blocking:
translation-profile = `'
disconnect-cause = `no-service'
advertise 0x40 capacity_update_timer 25 addrFamily 4 oldAddrFamily 4
mailbox selection policy: none
type = voip, session-target = `',
technology prefix:
settle-call = disabled
ip media DSCP = ef, ip media rsvp-pass DSCP = ef
```

```
ip media rsvp-fail DSCP = ef, ip signaling DSCP = af31,
ip video rsvp-none DSCP = af41,ip video rsvp-pass DSCP = af41
ip video rsvp-fail DSCP = af41,
ip defending Priority = 0, ip preemption priority = 0
ip policy locator voice:
ip policy locator video:
UDP checksum = disabled,
session-protocol = sipv2, session-transport = system,
req-qos = best-effort, acc-qos = best-effort,
req-qos video = best-effort, acc-qos video = best-effort,
req-qos audio def bandwidth = 64, req-qos audio max bandwidth = 0,
req-qos video def bandwidth = 384, req-qos video max bandwidth = 0,
RTP dynamic payload type values: NTE = 101
Cisco: NSE=100, fax=96, fax-ack=97, dtmf=121, fax-relay=122
CAS=123, TTY=119, ClearChan=125, PCM switch over u-law=0,
A-law=8, GSMAMR-NB=117 iLBC=116, AAC-ld=114, iSAC=124
lmr_tone=0, nte_tone=0
h263+=118, h264=119
G726r16 using static payload
G726r24 using static payload
RTP comfort noise payload type = 19
fax rate = voice,   payload size =  20 bytes
fax protocol = system
fax-relay ecm enable
Fax Relay ans enabled
Fax Relay SG3-to-G3 Enabled (by system configuration)
fax NSF = 0xAD0051 (default)
codec = g729r8,   payload size =  20 bytes,
video codec = None
voice class codec = `'
voice class sip session refresh system
voice class sip rsvp-fail-policy voice post-alert mandatory keep-alive interval 30
voice class sip rsvp-fail-policy voice post-alert optional keep-alive interval 30
voice class sip rsvp-fail-policy video post-alert mandatory keep-alive interval 30
voice class sip rsvp-fail-policy video post-alert optional keep-alive interval 30
text relay = disabled
Media Setting = forking (disabled) flow-through (global)
Expect factor = 10, Icpif = 20,
Playout Mode is set to adaptive,
Initial 60 ms, Max 1000 ms
Playout-delay Minimum mode is set to default, value 40 ms
Fax nominal 300 ms
Max Redirects = 1, signaling-type = cas,
VAD = enabled, Poor QOV Trap = disabled,
Source Interface = NONE
voice class sip url = system,
voice class sip tel-config url = system,
voice class sip rel1xx = system,
voice class sip anat = system,
voice class sip outbound-proxy = "system",
voice class sip associate registered-number = system,
voice class sip asserted-id system,
voice class sip privacy system
voice class sip e911 = system,
voice class sip history-info = system,
voice class sip reset timer expires 183 = system,
voice class sip pass-thru headers = system,
voice class sip pass-thru content unsupp = system,
voice class sip pass-thru content sdp = system,
voice class sip copy-list = system,
voice class sip g729 annexb-all = system,
voice class sip early-offer forced = system,
voice class sip negotiate cisco = system,
voice class sip block 180 = system,
```

```
voice class sip block 183 = system,
voice class sip block 181 = system,
voice class sip preloaded-route = system,
voice class sip random-contact = system,
voice class sip random-request-uri validate = system,
voice class sip call-route p-called-party-id = system,
voice class sip call-route history-info = system,
voice class sip privacy-policy send-always = system,
voice class sip privacy-policy passthru = system,
voice class sip privacy-policy strip history-info = system,
voice class sip privacy-policy strip diversion = system,
voice class sip map resp-code 181 = system,
voice class sip bind control = enabled, 9.42.28.29,
voice class sip bind media = enabled, 9.42.28.29,
voice class sip bandwidth audio = system,
voice class sip bandwidth video = system,
voice class sip encap clear-channel = system,
voice class sip error-code-override options-keepalive failure = system,
voice class sip calltype-video = false
voice class sip registration passthrough = System
voice class sip authenticate redirecting-number  = system,
redirect ip2ip = disabled
local peer = false
probe disabled,
Secure RTP: system (use the global setting)
voice class perm tag = `'
Time elapsed since last clearing of voice call statistics never
Connect Time = 0, Charged Units = 0,
Successful Calls = 0, Failed Calls = 0, Incomplete Calls = 0
Accepted Calls = 0, Refused Calls = 0,
Last Disconnect Cause is "",
Last Disconnect Text is "",
Last Setup Time = 0.
Last Disconnect Time = 0.

When there is no Dial-peer level bind -
voice class sip bind control = system,
voice class sip bind media = system,
```

The following is sample output from the **show dial-peer voice summary** command that shows connected FXO port 0/2/0 (the last entry) has OUT STAT set to “up,” which indicates that the POTS dial peer can be used for an outgoing call. If this port is disconnected, the status changes in the output so that the OUT STAT field reports “down,” and the POTS dial peer cannot be used for an outgoing call.

Note Beginning in Cisco IOS Release 15.1(3)T, there is improved status monitoring of FXO ports—any time an FXO port is connected or disconnected, a message is displayed to indicate the status change. For example, the following message is displayed to report that a cable has been connected, and the status is changed to “up” for FXO port 0/2/0:

```
000118: Jul 14 18:06:05.122 EST: %LINK-3-UPDOWN: Interface Foreign Exchange Office 0/2/0,
changed state to operational status up due to cable reconnection
```

```
Router# show dial-peer voice summary

dial-peer hunt 0
              AD                                      PRE PASS                 OUT
TAG    TYPE  MIN  OPER PREFIX    DEST-PATTERN      FER THRU SESS-TARGET    STAT PORT
KEEPALIVE
39275- voip  up   up             .T                 0  syst ipv4:172.18.108.26
82
```

```
8880    pots  up    up              8880              0                    up    2/0/0
8881    pots  up    up              8881              0                    up    2/0/1
8882    pots  up    up              8882              0                    up    2/0/2
8883    pots  up    up              8883              0                    up    2/0/3
8884    pots  up    up              8884              0                    up    2/0/4
8885    pots  up    up              8885              0                    up    2/0/5
8886    pots  up    up              8886              0                    up    2/0/6
8887    pots  up    up              8887              0                    up    2/0/7
88888-  pots  up    up                                0                  down  0/3/0:23
888
65033-  pots  up    up              6503352           0                    up    0/2/0
52
```

Table 70 describes the significant fields shown in the displays, in alphabetical order.

Table 70 show dial-peer voice Field Descriptions

Field	Description
Accepted Calls	Number of calls accepted from this peer since system startup.
acc-qos	Lowest acceptable quality of service configured for calls for this peer.
Admin state	Administrative state of this peer.
answer-address	Answer address configured for this dial peer.
bandwidth maximum/minimum	The maximum and minimum bandwidth, in Kb/s.
Charged Units	Total number of charging units that have applied to this peer since system startup, in hundredths of a second.
CLID Restriction	Indicates if Calling Line ID (CLID) restriction is enabled.
CLID Network Number	Displays the network number sent as CLID, if configured.
CLID Second Number sent	Displays whether a second calling number is stripped from the call setup.
CLID Override RDNIS	Indicates whether the CLID is overridden by the redirecting number.
codec	Default voice codec rate of speech.
Connect Time	Accumulated connect time to the peer since system startup for both incoming and outgoing calls, in hundredths of a second.
connections/maximum	Indicates the maximum number of call connections per peer.
Destination	Indicates the voice class that is used to match the destination URL.
destination-pattern	Destination pattern (telephone number) for this peer.
digit_strip	Indicates if digit stripping is enabled.
direct-inward-dial	Indicates if direct inward dial is enabled.
disconnect-cause	Indicates the disconnect cause code to be used when an incoming call is blocked.
dnis-map	Name of the dialed-number identification service (DNIS) map.
DTMF Relay	Indicates if dual-tone multifrequency (DTMF) relay is enabled.
Expect factor	User-requested expectation factor of voice quality for calls through this peer.
Failed Calls	Number of failed call attempts to this peer since system startup.

Table 70 show dial-peer voice Field Descriptions (continued)

Field	Description
fax rate	Fax transmission rate configured for this peer.
forward-digits	Indicates the destination digits to be forwarded of this peer.
group	Group number associated with this peer.
huntstop	Indicates whether dial-peer hunting is turned on, by the **huntstop** command, for this dial peer.
Icpif	Configured Impairment/Calculated Planning Impairment Factor (ICPIF) value for calls sent by a dial peer.
in bound application associated	Interactive voice response (IVR) application that is configured to handle inbound calls to this dial peer.
incall-number	Full E.164 telephone number to be used to identify the dial peer.
incoming call blocking	Indicates the incoming call blocking setup of this peer.
incoming called-number	Indicates the incoming called number if it has been set.
incoming COR list	Indicates the level of Class of Restrictions for incoming calls of this peer.
Incomplete Calls	Indicates the number of outgoing disconnected calls with the user busy (17), no user response (18), or no answer (19) cause code.
information type	Information type for this call (voice, fax, video).
Last Disconnect Cause	Encoded network cause associated with the last call. This value is updated whenever a call is started or cleared and depends on the interface type and session protocol being used on this interface.
Last Disconnect Text	ASCII text describing the reason for the last call termination.
Last Setup Time	Value of the system uptime when the last call to this peer was started.
Modem passthrough	Modem pass-through signaling method is named signaling event (NSE).
numbering Type	Indicates the numbering type for a peer call leg.
Operation state	Operational state of this peer.
outgoing COR list	Indicates the level of Class of Restrictions for outgoing calls of this peer.
outgoing LPCOR	Setting of the **lpcor outgoing** command.
out bound application associated	The voice application that is configured to handle outbound calls from this dial peer. Outbound calls are handed off to the named application.
Outbound state	Indicates the current outbound status of a POTS peer.
payload size	Indicates the size (in bytes) of the payload of the fax rate or codec setup.
payload type	NSE payload type.
peer type	Dial peer type (voice, data).
permission	Configured permission level for this peer.
Poor QOV Trap	Indicates if poor quality of voice trap messages is enabled.

Table 70 show dial-peer voice Field Descriptions (continued)

Field	Description
preemption level	Indicates the call preemption level of this peer.
prefix	Indicates dialed digits prefix of this peer.
Redundancy	Packet redundancy (RFC 2198) for modem traffic.
Refused Calls	Number of calls from this peer refused since system startup.
register E.164 number with H.323 GK and/or SIP Registrar	Indicates the "register e.164" option of this peer.
req-qos	Configured requested quality of service for calls for this dial peer.
session-target	Session target of this peer.
session-protocol	Session protocol to be used for Internet calls between local and remote routers through the IP backbone.
source carrier-id	Indicates the source carrier ID of this peer that will be used to match the source carrier ID of an incoming call.
source trunk-group label	Indicates the source trunk group label of this peer that can be used to match the source trunk group label of an incoming call.
Successful Calls	Number of completed calls to this peer.
supported-language	Indicates the list of supported languages of this peer.
tag	Unique dial peer ID number.
target carrier-id	Indicates the target carrier ID of this peer that will be used to match the target carrier ID for an outgoing call.
target-trunkgroup-label	Indicates the target trunk group label of this peer that can be used to match the target trunk group label of an outgoing call.
Time elapsed since last clearing of voice call statistics	Elapsed time between the current time and the time when the **clear dial-peer voice** command was executed.
Translation profile (Incoming)	Indicates the translation profile for incoming calls.
Translation profile (Outgoing)	Indicates the translation profile for outgoing calls.
translation-profile	Indicates the number translation profile of this peer.
type	Indicates the peer encapsulation type (pots, voip, vofr, voatm or mmoip).
VAD	Whether voice activation detection (VAD) is enabled for this dial peer.
voice class called-number inbound/outbound	Indicates the voice-class called number inbound or outbound setup of this peer.
voice class sip history-info	Indicates the configuration state of the history-info header. If the history-info header is not configured for the dial peer, this field is set to system. If the history-info header is enabled on this dial peer, this field is set to enable. If the history-info header is disabled on this dial peer, this field is set to disable.

Table 70 show dial-peer voice Field Descriptions (continued)

Field	Description
voice class sip bind	Indicates the configuration state of the bind address. If the bind is configured for the global, this field is sent to system. If the bind address is enabled on this dial peer, this field is set to enabled.
voice-port	Indicates the voice interface setting of this POTS peer.

The following is sample output from this command with the **summary** keyword:

```
Router# show dial-peer voice summary

dial-peer hunt 0
                                                        PASS
  TAG TYPE   ADMIN OPER PREFIX   DEST-PATTERN     PREF THRU SESS-TARGET    PORT
  100 pots   up    up                             0
  101 voip   up    up            5550112          0   syst ipv4:10.10.1.1
  102 voip   up    up            5550134          0   syst ipv4:10.10.1.1
   99 voip   up    down                           0   syst
   33 pots   up    down                           0
```

Table 71 describes the significant fields shown in the display.

Table 71 show dial-peer voice summary Field Descriptions

Field	Description
dial-peer hunt	Hunt group selection order that is defined for the dial peer by the **dial-peer hunt** command.
TAG	Unique identifier assigned to the dial peer when it was created.
TYPE	Type of dial peer (mmoip, pots, voatm, vofr, or voip).
ADMIN	Whether the administrative state is up or down.
OPER	Whether the operational state is up or down.
PREFIX	Prefix that is configured in the dial peer by the **prefix** command.
DEST-PATTERN	Destination pattern that is configured in the dial peer by the **destination-pattern** command.
PREF	Hunt group preference that is configured in the dial peer by the **preference** command.
PASS THRU	Modem pass-through method that is configured in the dial peer by the **modem passthrough** command.
SESS-TARGET	Destination that is configured in the dial peer by the **session target** command.
PORT	Router voice port that is configured for the dial peer. Valid only for POTS dial peers.

Related Commands

Command	Description
show call active voice	Displays the VoIP active call table.
show call history voice	Displays the VoIP call history table.

Command	Description
show dialplan incall number	Displays which POTS dial peer is matched for a specific calling number or voice port.
show dialplan number	Displays which dial peer is reached when a specific telephone number is dialed.
show num-exp	Displays how the number expansions are configured in VoIP.
show voice port	Displays configuration information about a specific voice port.

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 72 describes the significant fields shown in the display.

Table 72 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 eigrp address-family accounting

To display prefix accounting information for Enhanced Interior Gateway Routing Protocol (EIGRP) processes, use the **show eigrp address-family accounting** command in user EXEC or privileged EXEC mode.

show eigrp address-family {**ipv4** | **ipv6**} [**vrf** *vrf-name*] [*autonomous-system-number*] [**multicast**] **accounting**

Syntax Description

ipv4	Selects the IPv4 protocol address family.
ipv6	Selects the IPv6 protocol address family.
vrf *vrf-name*	(Optional) Displays information about the specified VRF. This keyword/argument pair is available only for IPv4 configurations.
autonomous-system-number	(Optional) Autonomous system number.
multicast	(Optional) Displays information about multicast instances.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command Default

Prefix accounting information for all EIGRP processes is displayed.

Command History

Release	Modification
15.0(1)M	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

This command can be used to display information about EIGRP named configurations and EIGRP autonomous-system (AS) configurations.

This command displays the same information as the **show ip eigrp accounting** command. Cisco recommends using the **show eigrp address-family accounting** command.

Examples

The following example shows how to display EIGRP prefix accounting information for autonomous-system 22:

```
Router# show eigrp address-family ipv4 22 accounting

EIGRP-IPv4 VR(saf) Accounting for AS(22)/ID(10.0.0.1)
Total Prefix Count: 3  States: A-Adjacency, P-Pending, D-Down
State Address/Source    Interface       Prefix   Restart  Restart/
```

```
                                                Count      Count    Reset(s)
A     10.0.0.2          Et0/0                     2          0          0
P     10.0.2.4          Se2/0                     0          2        114
D     10.0.1.3          Et0/0                     0          3          0
```

Table 73 describes the significant fields shown in the display.

Table 73 show eigrp address-family accounting Field Descriptions

Field	Description
IP-EIGRP accounting for AS...	Identifies the EIGRP instance, AS number, router ID, and table ID.
Total Prefix Count	Number of distinct prefixes that are present in this autonomous system.
State	State of the given neighbor: Adjacency, Pending, or Down.
Address/Source	IP address of the neighbor.
Interface	Interface on which the neighbor is connected.
Prefix Count	Number of prefixes that are advertised by this neighbor.
Restart Count	Number of times this neighbor has been restarted due to exceeding prefix limits.
Restart/Reset(s)	Time remaining until the neighbor will be restarted (if in Pending state) or until the restart count will be cleared (if in Adjacency state.)

Related Commands

Command	Description
show eigrp address-family events	Displays information about EIGRP events.
show eigrp address-family interfaces	Displays information about interfaces configured for EIGRP.
show eigrp address-family neighbors	Displays the neighbors discovered by EIGRP.
show eigrp address-family sia-event	Displays information about EIGRP SIA events.
show eigrp address-family sia-statistics	Displays information about EIGRP SIA statistics.
show eigrp address-family timers	Displays information about EIGRP timers and expiration times.
show eigrp address-family topology	Displays entries in the EIGRP topology table.
show eigrp address-family traffic	Displays the number of EIGRP packets sent and received.

show eigrp address-family events

To display information about Enhanced Interior Gateway Routing Protocol (EIGRP) address-family events, use the **show eigrp address-family events** command in user EXEC or privileged EXEC mode.

show eigrp address-family {**ipv4** | **ipv6**} [**vrf** *vrf-name*] [*autonomous-system-number*] [**multicast**] **events** [*starting-event-number ending-event-number*] [**errmsg** [*starting-event-number ending-event-number*]] [**sia** [*starting-event-number ending-event-number*]] [**type**]

Syntax Description

ipv4	Selects the IPv4 protocol address family.
ipv6	Selects the IPv6 protocol address family.
vrf *vrf-name*	(Optional) Displays information about the specified VRF.
autonomous-system-number	(Optional) Autonomous system number.
multicast	(Optional) Displays information about multicast instances.
starting-event-number	(Optional) Number of first event to display.
ending-event-number	(Optional) Number of last event to display.
errmsg	(Optional) Displays error message events.
sia	(Optional) Displays Stuck in Active (SIA) events.
type	(Optional) Displays the types of events being logged.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command Default

All EIGRP address-family events are displayed.

Command History

Release	Modification
15.0(1)M	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

The event log is used by Cisco technical support to display a history of EIGRP internal events that are specific to a particular address family.

To display information about EIGRP service-family events, use the **show eigrp service-family events** command.

This command can be used to display information about EIGRP named configurations and EIGRP autonomous-system (AS) configurations.

This command displays the same information as the **show ip eigrp events** command. Cisco recommends using the **show eigrp address-family events** command.

Examples

The following example shows how to display EIGRP address-family events for autonomous-system 3:

```
Router# show eigrp address-family ipv4 3 events

Event information for AS 3:
1 15:37:47.015 Change queue emptied, entries: 1
2 15:37:47.015 Metric set: 10.0.0.0/24 307200
3 15:37:47.015 Update reason, delay: new if 4294967295
4 15:37:47.015 Update sent, RD: 10.0.0.0/24 4294967295
5 15:37:47.015 Update reason, delay: metric chg 4294967295
6 15:37:47.015 Update sent, RD: 10.0.0.0/24 4294967295
7 15:37:47.015 Route installed: 10.0.0.0/24 1.1.1.2
8 15:37:47.015 Route installing: 10.0.0.0/24 10.0.1.2
```

Related Commands

Command	Description
show eigrp address-family accounting	Displays prefix accounting information for EIGRP processes.
show eigrp address-family interfaces	Displays information about interfaces configured for EIGRP.
show eigrp address-family neighbors	Displays the neighbors discovered by EIGRP.
show eigrp address-family sia-event	Displays information about EIGRP SIA events.
show eigrp address-family sia-statistics	Displays information about EIGRP SIA statistics.
show eigrp address-family timers	Displays information about EIGRP timers and expiration times.
show eigrp address-family topology	Displays entries in the EIGRP topology table.
show eigrp address-family traffic	Displays the number of EIGRP packets sent and received.
show eigrp service-family events	Displays information about EIGRP service-family events.

show eigrp address-family interfaces

To display information about interfaces that are configured for Enhanced Interior Gateway Routing Protocol (EIGRP), use the **show eigrp address-family interfaces** command in user EXEC or privileged EXEC mode.

show eigrp address-family {**ipv4** | **ipv6**} [**vrf** *vrf-name*] [*autonomous-system-number*] [**multicast**] **interfaces** [**detail**] [*interface-type interface-number*]

Syntax Description

ipv4	Selects the IPv4 protocol address family.
ipv6	Selects the IPv6 protocol address family.
vrf *vrf-name*	(Optional) Displays information about the specified VRF.
autonomous-system-number	(Optional) Autonomous system number.
multicast	(Optional) Displays information about multicast instances.
detail	(Optional) Displays detailed information about EIGRP interfaces.
interface-type interface-number	(Optional) Interface type and number to display. If unspecified, all enabled interfaces are displayed.

Command Default

All enabled EIGRP interfaces are displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

Use the **show eigrp address-family interfaces** command to determine on which interfaces EIGRP is active and to learn EIGRP information about those interfaces.

If an interface is specified, only information about that interface is displayed. Otherwise, information about all interfaces on which EIGRP is running is displayed.

If an autonomous system is specified, only the routing process for the specified autonomous system is displayed. Otherwise, all EIGRP processes are displayed.

This command can be used to display information about EIGRP named configurations and EIGRP autonomous-system (AS) configurations.

This command displays the same information as the **show ip eigrp interfaces** command. Cisco recommends using the **show eigrp address-family interfaces** command.

Examples

The following example shows how to display information about EIGRP interfaces for autonomous-system 4453:

```
Router# show eigrp address-family ipv4 4453 interfaces

EIGRP-IPv4 VR(Virtual-name) Address-family Neighbors for AS(4453)
                   Xmit Queue   Mean   Pacing Time   Multicast    Pending
Interface     Peers  Un/Reliable  SRTT   Un/Reliable   Flow Timer   Services
Se0           1          0/0        28      0/15          127           0
Se1           1          0/0        44      0/15          211           0
```

The following example shows how to display detailed information about Loopback interface 1 in autonomous-system 2:

```
Router# show eigrp address-family ipv4 2 interfaces detail Loopback1

EIGRP-IPv4 VR(saf2) Address-family Neighbors for AS(2)
                    Xmit Queue   Mean  Pacing Time     Multicast    Pending
Interface    Peers  Un/Reliable  SRTT  Un/Reliable     Flow Timer   Services
Lo1          166        0/0        48      0/1            258           0
    Hello-interval is 5, Hold-time is 15
    Split-horizon is enabled
    Next xmit serial <none>
    Un/reliable mcasts: 0/0 Un/reliable ucasts: 10148/67233
    Mcast exceptions: 0 CR packets: 0 ACKs suppressed: 8719
    Retransmissions sent: 2696 Out-of-sequence rcvd: 594
    Interface has all stub peers
    Topology-ids on interface - 0
    Authentication mode is not set
```

Table 74 describes the significant fields shown in the display.

Table 74 show eigrp address-family interfaces Field Descriptions

Field	Description
Interface	Interface over which EIGRP is configured.
Peers	Number of EIGRP neighbors connected on this interface.
Xmit Queue Un/Reliable	Number of packets remaining in the Unreliable and Reliable transmit queues.
Mean SRTT	Mean smooth round-trip time interval, in milliseconds.
Pacing Time Un/Reliable	Pacing time used to determine when reliable and unreliable EIGRP packets should be sent out of the interface.
Multicast Flow Timer	Maximum number of seconds the router sends multicast EIGRP packets.
Pending Services	Number of services in the packets in the transmit queue waiting to be sent.
CR packets	Packets marked for conditional Receive.

Related Commands

Command	Description
show eigrp address-family accounting	Displays prefix accounting information for EIGRP processes.
show eigrp address-family events	Displays information about EIGRP events.
show eigrp address-family neighbors	Displays the neighbors discovered by EIGRP.
show eigrp address-family sia-event	Displays information about EIGRP SIA events.
show eigrp address-family sia-statistics	Displays information about EIGRP SIA statistics.
show eigrp address-family timers	Displays information about EIGRP timers and expiration times.
show eigrp address-family topology	Displays entries in the EIGRP topology table.
show eigrp address-family traffic	Displays the number of EIGRP packets sent and received.

show eigrp address-family neighbors

To display the neighbors that are discovered by Enhanced Interior Gateway Routing Protocol (EIGRP), use the **show eigrp address-family neighbors** command in user EXEC or privileged EXEC mode.

show eigrp address-family {**ipv4** | **ipv6**} [**vrf** *vrf-name*] [*autonomous-system-number*] [**multicast**] **neighbors** [**static**] [**detail**] [*interface-type interface-number*]

Syntax Description

ipv4	Selects the IPv4 protocol address family.
ipv6	Selects the IPv6 protocol address family.
vrf *vrf-name*	(Optional) Displays information about the specified VRF.
autonomous-system-number	(Optional) Autonomous system number.
multicast	(Optional) Displays information about multicast instances.
static	(Optional) Displays static neighbors.
detail	(Optional) Displays detailed EIGRP neighbor information.
interface-type interface-number	(Optional) Interface type and number to display. If unspecified, all enabled interfaces are displayed.

Command Default

Information about all neighbors discovered by EIGRP is displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

Use the **show eigrp address-family neighbors** command to determine when neighbors become active and inactive. It is also useful for debugging certain types of transport problems.

This command can be used to display information about EIGRP named configurations and EIGRP autonomous-system (AS) configurations.

This command displays the same information as the **show ip eigrp neighbors** command. Cisco recommends using the **show eigrp address-family neighbors** command.

Examples

The following example shows how to display neighbors that are discovered by EIGRP:

```
Router# show eigrp address-family ipv4 4453 neighbors

EIGRP-IPv4 VR(Virtual-name) Address-family Neighbors for AS(4453)
Address                 Interface    Hold Uptime  SRTT  RTO    Q     Seq
                                       (sec)          (ms)  (ms)   Cnt   Num
172.16.81.28              Ethernet1     13   0:00:41  0      11   4     20
172.16.80.28              Ethernet0     14   0:02:01  0      10   12    24
172.16.80.31              Ethernet0     12   0:02:02  0      4    5     20
```

Table 75 describes the significant fields shown in the display.

The following example shows how to display detailed information about neighbors that are discovered by EIGRP, including whether a neighbor has been gracefully restarted:

```
Router# show eigrp address-family ipv4 neighbors detail

EIGRP-IPv4 VR(test) Address-Family Neighbors for AS(3)
H Address Interface Hold Uptime SRTT RTO Q Seq
                    (sec)       (ms) Cnt   Num
172.16.81.28 Et1/1 11 01:11:08 10 200 0 8
Time since Restart 00:00:05
Version 5.0/3.0, Retrans: 2, Retries: 0, Prefixes: 2
Topology-ids from peer - 0
```

Table 75 show eigrp address-family neighbors Field Descriptions

Field	Description
AS(4453)	Autonomous system number specified in the configuration command, in this example 4453.
Address	IP address of the peer.
Interface	Interface on which the router is receiving hello packets from the peer.
Hold time	Length of time, in seconds, that the router will wait to hear from the peer before declaring it down. If the peer is using the default hold time, this number will be less than 15. If the peer configures a nondefault hold time, it will be reflected here.
Uptime	Elapsed time since the local router first heard from this neighbor.
Q Cnt	Number of packets (update, query, and reply) that the software is waiting to send.
Seq Num	Sequence number of the last update, query, or reply packet that was received from this neighbor.
SRTT	Smooth round-trip time. This is the number of milliseconds that it takes for an EIGRP packet to be sent to this neighbor and for the local router to receive an acknowledgment of that packet.
RTO	Retransmission timeout, in milliseconds. Indicates the amount of time EIGRP waits before retransmitting a packet from the retransmission queue to a neighbor.
Time since Restart	Time elapsed since a neighbor has been gracefully restarted.

Related Commands

Command	Description
show eigrp address-family accounting	Displays prefix accounting information for EIGRP processes.
show eigrp address-family events	Displays information about EIGRP events.
show eigrp address-family interfaces	Displays information about interfaces configured for EIGRP.
show eigrp address-family sia-event	Displays information about EIGRP SIA events.
show eigrp address-family sia-statistics	Displays information about EIGRP SIA statistics.
show eigrp address-family timers	Displays information about EIGRP timers and expiration times.
show eigrp address-family topology	Displays entries in the EIGRP topology table.
show eigrp address-family traffic	Displays the number of EIGRP packets sent and received.

show eigrp address-family timers

To display information about Enhanced Interior Gateway Routing Protocol (EIGRP) timers and expiration times, use the **show eigrp address-family timers** command in user EXEC or privileged EXEC mode.

show eigrp address-family {**ipv4** | **ipv6**} [**vrf** *vrf-name*] [*autonomous-system-number*] [**multicast**] **timers**

Syntax Description

ipv4	Selects the IPv4 protocol address family.
ipv6	Selects the IPv6 protocol address family.
vrf *vrf-name*	(Optional) Displays information about the specified VRF.
autonomous-system-number	(Optional) Autonomous system number.
multicast	(Optional) Displays information about multicast instances.

Command Default

Information about all EIGRP timers is displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

This command is useful for debugging and troubleshooting by Cisco technical support, but it is not intended for normal EIGRP administration tasks. This command should not be used without guidance from Cisco technical support.

This command can be used to display information about EIGRP named configurations and EIGRP autonomous-system (AS) configurations.

This command displays the same information as the **show ip eigrp timers** command. Cisco recommends using the **show eigrp address-family timers** command.

Examples

The following example shows how to display information about EIGRP timers:

```
Router# show eigrp address-family ipv4 4453 timers

EIGRP-IPv4 VR(Virtual-name) Address-family Timers for AS(4453)
```

```
Hello Process
Expiration Type
| 1.022 (parent)
| 1.022 Hello (Et0/0)

Update Process
Expiration Type
| 14.984 (parent)
| 14.984 (parent)
| 14.984 Peer holding

SIA Process
Expiration Type for Topo(base)
| 0.000 (parent)
```

Related Commands

Command	Description
show eigrp address-family accounting	Displays prefix accounting information for EIGRP processes.
show eigrp address-family events	Displays information about EIGRP events.
show eigrp address-family interfaces	Displays information about interfaces configured for EIGRP.
show eigrp address-family neighbors	Displays the neighbors discovered by EIGRP.
show eigrp address-family sia-event	Displays information about EIGRP SIA events.
show eigrp address-family sia-statistics	Displays information about EIGRP SIA statistics.
show eigrp address-family topology	Displays entries in the EIGRP topology table.
show eigrp address-family traffic	Displays the number of EIGRP packets sent and received.

show eigrp address-family topology

To display entries in the Enhanced Interior Gateway Routing Protocol (EIGRP) topology table, use the **show eigrp address-family topology** command in user EXEC or privileged EXEC mode.

show eigrp address-family {**ipv4** | **ipv6**} [**vrf** *vrf-name*] [*autonomous-system-number*] [**multicast**] **topology** [*topology-name*] [*ip-address*] [**active**] [**all-links**] [**detail-links**] [**pending**] [**summary**] [**zero-successors**] [**route-type** {**connected** | **external** | **internal** | **local** | **redistributed** | **summary** | **vpn**}]

Syntax Description

ipv4	Selects the IPv4 protocol address family.
ipv6	Selects the IPv6 protocol address family.
vrf *vrf-name*	(Optional) Displays information about the specified VRF.
autonomous-system-number	(Optional) Specifies the autonomous system number.
multicast	(Optional) Displays information about multicast instances.
topology-name	(Optional) Named entry in the EIGRP topology table.
ip-address	(Optional) Network or network and mask. When specified, a detailed description of the entry is provided.
active	(Optional) Displays only active entries in the EIGRP topology table.
all-links	(Optional) Displays all entries in the EIGRP topology table (including non-feasible-successor sources).
detail-links	(Optional) Displays detailed information about all entries in the topology table.
pending	(Optional) Displays all entries in the EIGRP topology table that are waiting for an update from a neighbor or are waiting to reply to a neighbor.
summary	(Optional) Displays summary information about the EIGRP topology table.
zero-successors	(Optional) Displays available routes in the EIGRP topology table that have zero successors.
route-type	(Optional) Displays information about services of the specified route type.
connected	(Optional) Displays information about all connected routes.
external	(Optional) Displays information about all external routes.
internal	(Optional) Displays information about all internal routes.
local	(Optional) Displays information about all locally originated routes.
redistributed	(Optional) Displays information about all redistributed routes.
summary	(Optional) Displays information about all summary routes.
vpn	(Optional) Displays information about all VPN sourced routes. Applies to IPv4 only.

Command Default

If this command is used without any keywords or arguments, only routes that are feasible successors are displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

This command can be used to display information about EIGRP named configurations and EIGRP autonomous-system (AS) configurations.

This command displays the same information as the **show ip eigrp topology** command. Cisco recommends using the **show eigrp address-family topology** command.

Examples

The following example shows how to display entries in the EIGRP topology table:

```
Router# show eigrp address-family ipv4 4453 topology

EIGRP-IPv4 VR(Virtual-name) Topology Table for AS(4453)/ID(10.0.0.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status, s - sia Status
P  10.17.17.0/24, 1 successors, FD is 409600
          via 10.10.10.2 (409600/128256), Ethernet3/0
P  172.16.19.0/24, 1 successors, FD is 409600
          via 10.10.10.2 (409600/128256), Ethernet3/0
P  192.168.10.0/24, 1 successors, FD is 281600
          via Connected, Ethernet3/0
P  10.10.10.0/24, 1 successors, FD is 281600
          via Redistributed (281600/0)
```

The following example shows how to display EIGRP metrics for specified internal services and external services:

```
Router# show eigrp address-family ipv4 4453 topology 10.10.10.0/24

EIGRP-IPv4 VR(virtual-name) Topology Entry for AS(4453)/ID(10.0.0.1) for 10.10.10.0/24
  State is Passive, Query origin flag is 1, 1 Successor(s), FD is 128256
  Descriptor Blocks:
  0.0.0.0 (Null0), from Connected, Send flag is 0x0
      Composite metric is (128256/0), service is Internal
      Vector metric:
        Minimum bandwidth is 10000000 Kbit
        Total delay is 5000 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1514
        Hop count is 0
        Originating router is 10.0.0.1
```

Table 76 describes the significant fields shown in the display.

Table 76 show eigrp address-family topology Field Descriptions

Field	Description
Codes	State of this topology table entry. Passive and Active refer to the EIGRP state with respect to this destination; Update, Query, and Reply refer to the type of packet that is being sent.
P—Passive	No EIGRP computations are being performed for this destination.
A—Active	EIGRP computations are being performed for this destination.
U—Update	An update packet was sent to this destination.
Q—Query	A query packet was sent to this destination.
R—Reply	A reply packet was sent to this destination.
r—reply Status	Flag that is set after the software has sent a query and is waiting for a reply.
s—sia Status	Flag that is set if a route is in a stuck in active state.
successors	Number of successors. This number corresponds to the number of next hops in the IP routing table. If "successors" is capitalized, then the route or next hop is in a transition state.
FD	Feasible distance. The feasible distance is the best metric to reach the destination or the best metric that was known when the route went active. This value is used in the feasibility condition check. If the reported distance of the router (the metric after the slash) is less than the feasible distance, the feasibility condition is met and that path is a feasible successor. Once the software determines it has a feasible successor, it need not send a query for that destination.
replies	(Not shown in the output.) Number of replies that are still outstanding (have not been received) with respect to this destination. This information appears only when the destination is in the Active state.
state	(Not shown in the output) Exact EIGRP state that this destination is in. It can be the number 0, 1, 2, or 3. This information appears only when the destination is in the Active state.
via	IP address of the peer that told the software about this destination. The first N of these entries, where N is the number of successors, is the current successors. The remaining entries on the list are feasible successors.
(409600/128256)	The first number is the EIGRP metric that represents the cost to the destination. The second number is the EIGRP metric that this peer advertised.
Ethernet3/0	Interface from which this information was learned.

Related Commands

Command	Description
show eigrp address-family accounting	Displays prefix accounting information for EIGRP processes.
show eigrp address-family events	Displays information about EIGRP events.
show eigrp address-family interfaces	Displays information about interfaces configured for EIGRP.
show eigrp address-family neighbors	Displays the neighbors discovered by EIGRP.
show eigrp address-family sia-event	Displays information about EIGRP SIA events.
show eigrp address-family sia-statistics	Displays information about EIGRP SIA statistics.
show eigrp address-family timers	Displays information about EIGRP timers and expiration times.
show eigrp address-family traffic	Displays the number of EIGRP packets sent and received.

show eigrp address-family traffic

To display the number of Enhanced Interior Gateway Routing Protocol (EIGRP) packets that are sent and received, use the **show eigrp address-family traffic** command in user EXEC or privileged EXEC mode.

show eigrp address-family {**ipv4** | **ipv6**} [**vrf** *vrf-name*] [*autonomous-system-number*] [**multicast**] **traffic**

Syntax Description

ipv4	Selects the IPv4 protocol address family.
ipv6	Selects the IPv6 protocol address family.
vrf *vrf-name*	(Optional) Displays information about the specified VRF.
autonomous-system-number	(Optional) Autonomous system number.
multicast	(Optional) Displays information about multicast instances.

Command Default

The number of all EIGRP packets sent and received is displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

This command can be used to display information about EIGRP named configurations and EIGRP autonomous-system (AS) configurations.

This command displays the same information as the **show ip eigrp traffic** command. Cisco recommends using the **show eigrp address-family traffic** command.

Examples

The following example shows how to display the number of EIGRP packets sent and received for autonomous system number 4453:

```
Router# show eigrp address-family ipv4 4453 traffic

EIGRP-IPv4 VR(virtual-name) Address-family Traffic Statistics for AS(4453)
  Hellos sent/received: 122/122
  Updates sent/received: 3/1
  Queries sent/received: 0/0
```

```
Replies sent/received: 0/0
Acks sent/received: 0/3
SIA-Queries sent/received: 0/0
SIA-Replies sent/received: 0/0
Hello Process ID: 128
PDM Process ID: 191
Socket Queue: 0/2000/1/0 (current/max/highest/drops)
Input Queue: 0/2000/1/0 (current/max/highest/drops
```

Table 77 describes the significant fields shown in the display.

Table 77 show eigrp address-family traffic Field Descriptions

Field	Description
Hellos sent/received	Number of hello packets sent and received.
Updates sent/received	Number of update packets sent and received.
Queries sent/received	Number of query packets sent and received.
Replies sent/received	Number of reply packets sent and received.
Acks sent/received	Number of acknowledgement packets sent and received.
SIA-Queries sent/received	Number of stuck in active query packets sent and received.
SIA-Replies sent/received	Number of stuck in active reply packets sent and received.
Hello Process ID	Cisco IOS hello process identifier.
PDM Process ID	Protocol-dependent module IOS process identifier.
Socket Queue	IP to EIGRP Hello Process socket queue counters.
Input Queue	EIGRP Hello Process to EIGRP PDM socket queue counters.

Related Commands

Command	Description
show eigrp address-family accounting	Displays prefix accounting information for EIGRP processes.
show eigrp address-family events	Displays information about EIGRP events.
show eigrp address-family interfaces	Displays information about interfaces configured for EIGRP.
show eigrp address-family neighbors	Displays the neighbors discovered by EIGRP.
show eigrp address-family sia-event	Displays information about EIGRP SIA events.
show eigrp address-family sia-statistics	Displays information about EIGRP SIA statistics.
show eigrp address-family timers	Displays information about EIGRP timers and expiration times.
show eigrp address-family topology	Displays entries in the EIGRP topology table.

show erm statistics

To display the Embedded Resource Manager (ERM) Forwarding Information Base (FIB) ternary content addressable memory (TCAM) exception status for IPv4, IPv6, and Multiprotocol Label Switching (MPLS) protocols, use the **show erm statistics** command in privileged EXEC mode.

show erm statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(17b)SXA	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 IPv4, IPv6, and MPLS exception state displays FALSE when the protocol is not under the exception or displays TRUE when the protocol is under the exception.

Examples

This example shows how to display FIB TCAM exception status for IPv4, IPv6, and MPLS protocols:

```
Router# show erm statistics

#IPv4 excep notified     = 0
#IPv6 excep notified     = 0
#MPLS excep notified     = 0
#IPv4 reloads done       = 0
#IPv6 reloads done       = 0
#MPLS reloads done       = 0
Current IPv4 excep state = FALSE
Current IPv6 excep state = FALSE
Current MPLS excep state = FALSE
#Timer expired           = 0
#of erm msgs             = 1
```

Table 78 describes the significant fields shown in the display.

Table 78 show erm statistics Field Descriptions

Field	Description
... excep notified	The number of exceptions for each protocol.
... reloads done	The number of reloads for each protocol.
...Current *protocol* exception state	The current exception status of each protocol.
#of erm msgs	The number of ERM messages sent.

Related Commands

Command	Description
mls erm priority	Assigns the priorities to define an order in which protocols attempt to recover from the exception status.

show fm ipv6 pbr all

To display IPv6 policy-based routing (PBR) value mask results (VMRs), use the **show fm ipv6 pbr all** command in privileged EXEC mode.

show fm ipv6 pbr all

Syntax Description

This command has no arguments or keywords.

Command Default

PBR configuration is not displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(33)SXI4	This command was introduced.

Usage Guidelines

The **show fm ipv6 pbr all** command shows the IPv6 PBR VMRs for all interfaces with IPv6 PBR configured.

show fm ipv6 pbr interface

To displays the IPv6 policy-based routing (PBR) value mask results (VMRs) on a specified interface, use the **show fm ipv6 pbr interface** command in privileged EXEC mode.

show fm ipv6 pbr interface {**interface** *type number*}

Syntax Description

interface *type number*	Specified interface for which PBR VMR information will be displayed.

Command Default

PBR VMR information on an interface is not displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(33)SXI4	This command was introduced.

Usage Guidelines

The **show fm ipv6 pbr all** command shows the IPv6 PBR VMRs for a specified interface.

show fm ipv6 traffic-filter

To display the IPv6 information, use the **show fm ipv6 traffic-filter** command in privileged EXEC mode.

show fm ipv6 traffic-filter {**all** | **interface** *type number*}

Syntax Description

all	Displays IPv6 traffic filter information for all interfaces.
interface *type*	Displays IPv6 traffic filter information for the specified interface; possible valid values are **ethernet**, **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **pos**, **atm**, **ge-wan** and **vlan**.
number	Module and port number; see the "Usage Guidelines" section for valid values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(14)SX	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 12.2(33)SRA.

Usage Guidelines

The **pos**, **atm**, and **ge-wan** keywords are supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

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 how to display the IPv6 information for a specific interface:

```
Router# show fm ipv6 traffic-filter interface vlan 50

------------------------------------------------------------------------------
FM_FEATURE_IPV6_ACG_INGRESS Name:testipv6 i/f: Vlan50
==============================================================================
DPort - Destination Port SPort - Source Port Pro - Protocol
X - XTAG TOS - TOS Value Res - VMR Result
RFM - R-Recirc. Flag MRTNP - M-Multicast Flag R - Reflexive flag
- F-Fragment flag - T-Tcp Control N - Non-cachable
- M-More Fragments - P-Mask Priority(H-High, L-Low)
Adj. - Adj. Index T - M(Mask)/V(Value) FM - Flow Mask
```

```
NULL - Null FM SAO - Source Only FM DAO - Dest. Only FM
SADA - Sour.& Dest. Only VSADA - Vlan SADA Only FF - Full Flow
VFF - Vlan Full Flow F-VFF - Either FF or VFF A-VSD - Atleast VSADA
A-FF - Atleast FF A-VFF - Atleast VFF A-SON - Atleast SAO
A-DON - Atleast DAO A-SD - Atleast SADA SHORT - Shortest
A-SFF - Any short than FF A-EFF - Any except FF A-EVFF- Any except VFF
A-LVFF- Any less than VFF ERR - Flowmask Error
+----+-+---------------------------------------+---------------------------------------+
---+---+-+-----+----+------+
|Indx|T| Dest IPv6 Addr | Source IPv6
Addr |Pro|RFM|X|MRTNP|Adj.| FM |
+----+-+---------------------------------------+---------------------------------------+
---+---+-+-----+----+------+
1 V 0:200E::
200D::1 0 -F- - ----L ---- Shorte
M 0:FFFF:FFFF:FFFF:FFFF::
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF 0 1
TM_SOFT_BRIDGE_RESULT
2 V 0:200E::
200D::1 17 --- - ----L ---- Shorte
M 0:FFFF:FFFF:FFFF:FFFF::
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF 255 0
TM_PERMIT_RESULT
3 V 200E::
200D::1 0 -F- - ----L ---- Shorte
M FFFF:FFFF:FFFF:FFFF::
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF 0 1
TM_SOFT_BRIDGE_RESULT
4 V 200E::
200D::1 17 --- - ----L ---- Shorte
M FFFF:FFFF:FFFF:FFFF::
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF 255 0
TM_PERMIT_RESULT
5 V
:: :: 0 -F- - ----L ---- Shorte
M
:: :: 0 1
TM_SOFT_BRIDGE_RESULT
6 V
:: :: 0 -F- - ----L ---- Shorte
M
:: :: 0 1
TM_SOFT_BRIDGE_RESULT
7 V
:: :: 58 --- - ----L ---- Shorte
M
:: :: 255 0
TM_PERMIT_RESULT
8 V
:: :: 58 --- - ----L ---- Shorte
M
:: :: 255 0
TM_PERMIT_RESULT
9 V
:: :: 58 --- - ----L ---- Shorte
M
:: :: 255 0
```

```
TM_PERMIT_RESULT
10 V
:: :: 58 --- - ----L ---- Shorte
M
:: :: 255 0
TM_PERMIT_RESULT
11 V
:: :: 58 --- - ----L ---- Shorte
M
:: :: 255 0
TM_PERMIT_RESULT
12 V
:: :: 58 --- - ----L ---- Shorte
M
:: :: 255 0
TM_PERMIT_RESULT
13 V
:: :: 58 --- - ----L ---- Shorte
M
:: :: 255 0
TM_PERMIT_RESULT
14 V
:: :: 58 --- - ----L ---- Shorte
M
:: :: 255 0
TM_PERMIT_RESULT
15 V
:: :: 0 --- - ----L ---- Shorte
M
:: :: 0 0
TM_L3_DENY_RESULT
Router#
```

This example shows how to display the IPv6 information for all interfaces:

```
Router# show fm ipv6 traffic-filter all

------------------------------------------------------------------------------
FM_FEATURE_IPV6_ACG_INGRESS Name:testipv6 i/f: Vlan50
==============================================================================
DPort - Destination Port SPort - Source Port Pro - Protocol
X - XTAG TOS - TOS Value Res - VMR Result
RFM - R-Recirc. Flag MRTNP - M-Multicast Flag R - Reflexive flag
- F-Fragment flag - T-Tcp Control N - Non-cachable
- M-More Fragments - P-Mask Priority(H-High, L-Low)
Adj. - Adj. Index T - M(Mask)/V(Value) FM - Flow Mask
NULL - Null FM SAO - Source Only FM DAO - Dest. Only FM
SADA - Sour.& Dest. Only VSADA - Vlan SADA Only FF - Full Flow
VFF - Vlan Full Flow F-VFF - Either FF or VFF A-VSD - Atleast VSADA
A-FF - Atleast FF A-VFF - Atleast VFF A-SON - Atleast SAO
A-DON - Atleast DAO A-SD - Atleast SADA SHORT - Shortest
A-SFF - Any short than FF A-EFF - Any except FF A-EVFF- Any except VFF
A-LVFF- Any less than VFF ERR - Flowmask Error
+----+-+---------------------------------------+---------------------------------------+
---+---+-+-----+----+------+
```

```
|Indx|T| Dest IPv6 Addr | Source IPv6
Addr |Pro|RFM|X|MRTNP|Adj.| FM |
+----+-+---------------------------------------+---------------------------------------+
---+---+-+-----+----+------+
1 V 0:200E::
200D::1 0 -F- - ----L ---- Shorte
M 0:FFFF:FFFF:FFFF:FFFF::
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF 0 1
TM_SOFT_BRIDGE_RESULT
2 V 0:200E::
200D::1 17 --- - ----L ---- Shorte
M 0:FFFF:FFFF:FFFF:FFFF::
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF 255 0
TM_PERMIT_RESULT
3 V 200E::
200D::1 0 -F- - ----L ---- Shorte
M FFFF:FFFF:FFFF:FFFF::
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF 0 1
TM_SOFT_BRIDGE_RESULT
4 V 200E::
200D::1 17 --- - ----L ---- Shorte
M FFFF:FFFF:FFFF:FFFF::
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF 255 0
TM_PERMIT_RESULT
5 V
:: :: 0 -F- - ----L ---- Shorte
M
:: :: 0 1
TM_SOFT_BRIDGE_RESULT
6 V
:: :: 0 -F- - ----L ---- Shorte
M
:: :: 0 1
TM_SOFT_BRIDGE_RESULT
7 V
:: :: 58 --- - ----L ---- Shorte
M
:: :: 255 0
TM_PERMIT_RESULT
8 V
:: :: 58 --- - ----L ---- Shorte
M
:: :: 255 0
TM_PERMIT_RESULT
9 V
:: :: 58 --- - ----L ---- Shorte
M
:: :: 255 0
TM_PERMIT_RESULT
10 V
:: :: 58 --- - ----L ---- Shorte
M
:: :: 255 0
13 V
:: :: 58 --- - ----L ---- Shorte
M
:: :: 255 0
.
. Output is truncated
.
Interface(s) using this IPv6 Ingress Traffic Filter:
Vl50,
```

show fm raguard

To display the interfaces configured with router advertisement (RA) guard, use the **show fm raguard** command in privileged EXEC mode.

show fm raguard

Syntax Description

This command has no arguments or keywords.

Command Default

RA guard interface information is not displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(33)SXI4	This command was introduced.
12.2(54)SG	This command was modified. Support for Cisco IOS Release 12.2(54)SG was added.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

Use the **show fm raguard** command to verify information about interfaces that are configured with RA guard.

Examples

The following example enables the display of interfaces configured with IPv6 RA guard:

```
Router# show fm raguard

------------------------------------------------------------------------------
 IPV6 RA GUARD in Ingress direction is configured on following interfaces
==============================================================================
Interface: Port-channel23
Interface: GigabitEthernet4/6
```

Table 79 describes the significant fields shown in the display.

Table 79 show fm raguard Field Descriptions

Field	Description
IPV6 RA GUARD in Ingress direction is configured on following interfaces	Displays the interfaces configured with IPv6 RA guard.

show frame-relay lmi

To display statistics about the Local Management Interface (LMI), use the **show frame-relay lmi** command in user EXEC or privileged EXEC mode.

show frame-relay lmi [*type number*]

Syntax Description

type	(Optional) Interface type; it must be **serial**.
number	(Optional) Interface number.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(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.
12.0(33)S	Support for IPv6 was added. This command was implemented on the Cisco 12000 series routers.

Usage Guidelines

Enter the command without arguments to obtain statistics about all Frame Relay interfaces.

Examples

The following is sample output from the **show frame-relay lmi** command when the interface is a data terminal equipment (DTE) device:

```
Router# show frame-relay lmi

LMI Statistics for interface Serial1 (Frame Relay DTE) LMI TYPE = ANSI
  Invalid Unnumbered info 0             Invalid Prot Disc 0
  Invalid dummy Call Ref 0              Invalid Msg Type 0
  Invalid Status Message 0              Invalid Lock Shift 0
  Invalid Information ID 0              Invalid Report IE Len 0
  Invalid Report Request 0              Invalid Keep IE Len 0
  Num Status Enq. Sent 9                Num Status msgs Rcvd 0
  Num Update Status Rcvd 0              Num Status Timeouts 9
```

The following is sample output from the **show frame-relay lmi** command when the interface is a Network-to-Network Interface (NNI):

```
Router# show frame-relay lmi

LMI Statistics for interface Serial3 (Frame Relay NNI) LMI TYPE = CISCO
  Invalid Unnumbered info 0             Invalid Prot Disc 0
  Invalid dummy Call Ref 0              Invalid Msg Type 0
  Invalid Status Message 0              Invalid Lock Shift 0
```

```
Invalid Information ID 0              Invalid Report IE Len 0
Invalid Report Request 0              Invalid Keep IE Len 0
Num Status Enq. Rcvd 11               Num Status msgs Sent 11
Num Update Status Rcvd 0              Num St Enq. Timeouts 0
Num Status Enq. Sent 10               Num Status msgs Rcvd 10
Num Update Status Sent 0              Num Status Timeouts 0
```

Table 80 describes significant fields shown in the output.

Table 80 show frame-relay lmi Field Descriptions

Field	Description
LMI Statistics	Signalling or LMI specification: CISCO, ANSI, or ITU-T.
Invalid Unnumbered info	Number of received LMI messages with invalid unnumbered information field.
Invalid Prot Disc	Number of received LMI messages with invalid protocol discriminator.
Invalid dummy Call Ref	Number of received LMI messages with invalid dummy call references.
Invalid Msg Type	Number of received LMI messages with invalid message type.
Invalid Status Message	Number of received LMI messages with invalid status message.
Invalid Lock Shift	Number of received LMI messages with invalid lock shift type.
Invalid Information ID	Number of received LMI messages with invalid information identifier.
Invalid Report IE Len	Number of received LMI messages with invalid Report IE Length.
Invalid Report Request	Number of received LMI messages with invalid Report Request.
Invalid Keep IE Len	Number of received LMI messages with invalid Keep IE Length.
Num Status Enq. Sent	Number of LMI status inquiry messages sent.
Num Status Msgs Rcvd	Number of LMI status messages received.
Num Update Status Rcvd	Number of LMI asynchronous update status messages received.
Num Status Timeouts	Number of times the status message was not received within the keepalive time value.
Num Status Enq. Rcvd	Number of LMI status enquiry messages received.
Num Status Msgs Sent	Number of LMI status messages sent.
Num Status Enq. Timeouts	Number of times the status enquiry message was not received within the T392 DCE timer value.
Num Update Status Sent	Number of LMI asynchronous update status messages sent.

show frame-relay map

To display current Frame Relay map entries and information about connections, use the **show frame-relay map** command in privileged EXEC mode.

show frame-relay map [**interface** *type number*] [*dlci*]

Syntax Description

interface *type number*	(Optional) Specifies an interface for which mapping information will be displayed. A space is optional between the interface type and number.
dlci	(Optional) Specifies a data-link connection identifier (DLCI) for which mapping information will be displayed. Range: 16 to 1022.

Command Default

Static and dynamic Frame Relay map entries and information about connections for all DLCIs on all interfaces are displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(2)T	The display output for this command was modified to include the IPv6 address mappings of remote nodes to Frame Relay permanent virtual circuits (PVCs).
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 Release 12.2(14)S.
12.2(13)T	The display output for this command was modified to include information about Frame Relay PVC bundle maps.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB, the **interface** keyword was added, and the *dlci* argument was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(9)T	The **interface** keyword was added, and the *dlci* argument 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.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
12.0(33)S	This command was implemented on the Cisco 12000 series routers.

Examples

This section contains the following examples:

- Display All Maps or Maps for Specific DLCIs on Specific Interfaces or Subinterfaces: Example, page 1587

Display All Maps or Maps for Specific DLCIs on Specific Interfaces or Subinterfaces: Example

The sample output in these examples uses the following configuration:

```
interface POS2/0
 no ip address
 encapsulation frame-relay
 frame-relay map ip 10.1.1.1 20 tcp header-compression
 frame-relay map ip 10.1.2.1 21 tcp header-compression
 frame-relay map ip 10.1.3.1 22 tcp header-compression
 frame-relay map bridge 23
 frame-relay interface-dlci 25
 frame-relay interface-dlci 26
 bridge-group 1
interface POS2/0.1 point-to-point
 frame-relay interface-dlci 24 protocol ip 10.1.4.1

interface Serial3/0
 no ip address
 encapsulation frame-relay
 serial restart-delay 0
 frame-relay map ip 172.16.3.1 20
 frame-relay map ip 172.16.4.1 21 tcp header-compression active
 frame-relay map ip 172.16.1.1 100
 frame-relay map ip 172.16.2.1 101
interface Serial3/0.1 multipoint
 frame-relay map ip 192.168.11.11 24
 frame-relay map ip 192.168.11.22 105
```

The following example shows how to display all maps:

```
Router# show frame-relay map

POS2/0 (up): ip 10.1.1.1 dlci 20(0x14,0x440), static,
              CISCO, status deleted
              TCP/IP Header Compression (enabled), connections: 256
POS2/0 (up): ip 10.1.2.1 dlci 21(0x15,0x450), static,
              CISCO, status deleted
              TCP/IP Header Compression (enabled), connections: 256
POS2/0 (up): ip 10.1.3.1 dlci 22(0x16,0x460), static,
              CISCO, status deleted
              TCP/IP Header Compression (enabled), connections: 256
POS2/0 (up): bridge dlci 23(0x17,0x470), static,
              CISCO, status deleted
POS2/0.1 (down): point-to-point dlci, dlci 24(0x18,0x480), broadcast
          status deleted
Serial3/0 (downup): ip 172.16.3.1 dlci 20(0x14,0x440), static,
              CISCO, status deleted
Serial3/0 (downup): ip 172.16.4.1 dlci 21(0x15,0x450), static,
              CISCO, status deleted
              TCP/IP Header Compression (enabled), connections: 256
Serial3/0.1 (downup): ip 192.168.11.11 dlci 24(0x18,0x480), static,
              CISCO, status deleted
Serial3/0 (downup): ip 172.16.1.1 dlci 100(0x64,0x1840), static,
              CISCO, status deleted
Serial3/0 (downup): ip 172.16.2.1 dlci 101(0x65,0x1850), static,, CISCO,
              CISCO, status deleted
              ECRTP Header Compression (enabled, IETF), connections 16
              TCP/IP Header Compression (enabled, IETF), connections 16
Serial3/0.1 (downup): ip 192.168.11.22 dlci 105(0x69,0x1890), static,
              CISCO, status deleted
```

```
Serial4/0/1:0.1 (up): point-to-point dlci, dlci 102(0x66,0x1860), broadcast, CISCO
          status defined, active,
              RTP Header Compression (enabled), connections: 256
```

The following example shows how to display maps for a specific DLCI:

```
Router# show frame-relay map 20

POS2/0 (up): ip 10.1.1.1 dlci 20(0x14,0x440), static,
              CISCO, status deleted
              TCP/IP Header Compression (enabled), connections: 256
Serial3/0 (down): ip 172.16.3.1 dlci 20(0x14,0x440), static,
              CISCO, status deleted
```

The following example shows how to display maps for a specific interface:

```
Router# show frame-relay map interface pos2/0

POS2/0 (up): ip 10.1.1.1 dlci 20(0x14,0x440), static,
              CISCO, status deleted
              TCP/IP Header Compression (enabled), connections: 256
POS2/0 (up): ip 10.1.2.1 dlci 21(0x15,0x450), static,
              CISCO, status deleted
              TCP/IP Header Compression (enabled), connections: 256
POS2/0 (up): ip 10.1.3.1 dlci 22(0x16,0x460), static,
              CISCO, status deleted
              TCP/IP Header Compression (enabled), connections: 256
POS2/0 (up): bridge dlci 23(0x17,0x470), static,
              CISCO, status deleted
POS2/0.1 (down): point-to-point dlci, dlci 24(0x18,0x480), broadcast
          status deleted
```

The following example shows how to display maps for a specific DLCI on a specific interface:

```
Router# show frame-relay map interface pos2/0 20

POS2/0 (up): ip 10.1.1.1 dlci 20(0x14,0x440), static,
              CISCO, status deleted
              TCP/IP Header Compression (enabled), connections: 256
```

The following example shows how to display maps for a specific subinterface:

```
Router# show frame-relay map interface pos2/0.1

POS2/0.1 (down): point-to-point dlci, dlci 24(0x18,0x480), broadcast
          status deleted
```

The following example shows how to display maps for a specific DLCI on a specific subinterface:

```
Router# show frame-relay map interface pos2/0.1 24

POS2/0.1 (down): point-to-point dlci, dlci 24(0x18,0x480), broadcast
          status deleted
```

Display Maps for PVC Bundles: Example

The sample output in this example uses the following router configuration:

```
hostname router1
!
interface Serial2/0
 ip address 10.0.0.2 255.255.255.0
 encapsulation frame-relay
 frame-relay vc-bundle vcb1
  pvc 100 vcb1-classA
   precedence 1-7
```

```
   class vcb1-classA
  pvc 109 vcb1-others
   precedence other
   class others
 frame-relay intf-type dce
!
map-class frame-relay vcb1-classA
 frame-relay cir 128000
!
map-class frame-relay others
 frame-relay cir 64000

hostname router2
!
interface Serial3/3
 ip address 10.0.0.1 255.255.255.0
 encapsulation frame-relay
 frame-relay vc-bundle vcb1
  pvc 100 vcb1-classA
   precedence 1-7
   class vcb1-classA
  pvc 109 vcb1-others
   precedence other
   class others
!
map-class frame-relay vcb1-classA
 frame-relay cir 128000
!
map-class frame-relay others
 frame-relay cir 64000
```

The following sample output displays mapping information for two PVC bundles. The PVC bundle MAIN-1-static is configured with a static map. The map for PVC bundle MAIN-2-dynamic is created dynamically using Inverse Address Resolution Protocol (ARP).

```
Router# show frame-relay map

Serial1/4 (up): ip 10.1.1.1 vc-bundle MAIN-1-static, static,
          CISCO, status up
Serial1/4 (up): ip 10.1.1.2 vc-bundle MAIN-2-dynamic, dynamic,
          broadcast, status up
```

Display Maps for IPv6 Addresses: Example

The sample output in this example uses the following router configuration:

```
hostname router1
!
interface Serial2/0
 no ip address
 encapsulation frame-relay
!
interface Serial2/0.1 point-to-point
 ipv6 address 1::1/64
 frame-relay interface-dlci 101
!
interface Serial2/0.2 multipoint
 ipv6 address 2::1/64
 frame-relay map ipv6 2::2 201
 frame-relay interface-dlci 201
!

hostname router2
!
```

```
interface Serial3/3
 no ip address
 encapsulation frame-relay
 frame-relay intf-type dce
!
interface Serial3/3.1 point-to-point
 ipv6 address 1::2/64
 frame-relay interface-dlci 101
!
interface Serial3/3.2 multipoint
 ipv6 address 2::2/64
 frame-relay map ipv6 3::1 201
 frame-relay interface-dlci 201
!
```

The following sample output from the **show frame-relay map** command shows that the link-local and global IPv6 addresses (FE80::E0:F727:E400:A and 2001:0DB8:2222:1044::32; FE80::60:3E47:AC8:8 and 2001:0DB8:2222:1044::32) of two remote nodes are explicitly mapped to DLCI 17 and DLCI 19, respectively. Both DLCI 17 and DLCI 19 are terminated on interface serial 3 of this node; therefore, interface serial 3 of this node is a point-to-multipoint interface.

```
Router# show frame-relay map

Serial3 (up): ipv6 FE80::E0:F727:E400:A dlci 17(0x11,0x410), static,
              broadcast, CISCO, status defined, active
Serial3 (up): ipv6 2001:0DB8:2222:1044::32 dlci 19(0x13,0x430), static,
              CISCO, status defined, active

Serial3 (up): ipv6 2001:0DB8:2222:1044::32 dlci 17(0x11,0x410), static,
              CISCO, status defined, active
Serial3 (up): ipv6 FE80::60:3E47:AC8:8 dlci 19(0x13,0x430), static,
              broadcast, CISCO, status defined, active
```

Table 81 describes the significant fields shown in the displays.

Table 81 show frame-relay map Field Descriptions

Field	Description
POS2/0 (up)	Identifies a Frame Relay interface and its status (up or down).
ip 10.1.1.1	Destination IP address.
dlci 20(0x14,0x440)	DLCI that identifies the logical connection being used to reach this interface. This value is displayed in three ways: its decimal value (20), its hexadecimal value (0x14), and its value as it would appear on the wire (0x440).
vc-bundle	PVC bundle that serves as the logical connection being used to reach the interface.
static/dynamic	Indicates whether this is a static or dynamic entry.
broadcast	Indicates pseudobroadcasting.
CISCO	Indicates the encapsulation type for this map: either CISCO or IETF.

Table 81 show frame-relay map Field Descriptions (continued)

Field	Description
TCP/IP Header Compression (inherited), passive (inherited)	Indicates the header compression type (TCP/IP, Real-Time Transport Protocol (RTP), or Enhanced Compressed Real-Time Transport Protocol (ECRTP)) and whether the header compression characteristics were inherited from the interface or were explicitly configured for the IP map.
status defined, active	Indicates that the mapping between the destination address and the DLCI used to connect to the destination address is active.

Related Commands

Command	Description
show frame-relay pvc	Displays statistics about PVCs for Frame Relay interfaces.
show frame-relay vc-bundle	Displays attributes and other information about a Frame Relay PVC bundle.

show frame-relay multilink

To display configuration information and statistics about multilink Frame Relay bundles and bundle links, use the **show frame-relay multilink** command in user EXEC or privileged EXEC mode.

show frame-relay multilink [**mfr** *number* | **serial** *number*] [**dlci** {*dlci-number* | **lmi**}] [**detailed**]

Syntax Description

mfr *number*	(Optional) Displays information about a specific bundle interface.
serial *number*	(Optional) Displays information about a specific bundle link interface.
dlci	(Optional) Displays information about the data-link connection identifier (DLCI).
dlci-number	DLCI number. The range is from 16 to 1022.
lmi	Displays information about the Local Management Interface (LMI) DLCI.
detailed	(Optional) Displays more-detailed information, including counters for the control messages sent to and from the peer device and the status of the bundle links.

Command Default

Information for all bundles and bundle links is displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(17)S	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(24)S	This command was implemented on VIP-enabled Cisco 7500 series routers.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(4)T	This command was implemented on VIP-enabled Cisco 7500 series routers.
12.0(30)S	This command was updated to display Multilink Frame Relay variable bandwidth class status.
12.4(2)T	This command was updated to display Multilink Frame Relay variable bandwidth class status.
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 was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.0(33)S	Support for IPv6 was added. This command was implemented on the Cisco 12000 series routers.

Examples

All Bundles and Bundle Links: Example

The following is sample output from the **show frame-relay multilink** command (see Table 82 for descriptions of the fields). Because a specific bundle or bundle link is not specified, information for all bundles and bundle links is displayed:

```
Router# show frame-relay multilink

Bundle:MFR0, State = up, class = A, fragmentation disabled
 BID = MFR0
 Bundle links :
 Serial2/1:3, HW state :up, Protocol state :Idle, LID :Serial2/1:3
 Serial2/1:2, HW state :up, Protocol state :Idle, LID :Serial2/1:2
 Serial2/1:1, HW state :up, Protocol state :Idle, LID :Serial2/1:1
```

The following is sample output from the **show frame-relay multilink** command when a Frame Relay bundle is configured as bandwidth class C (threshold) (see Table 82 for descriptions of the fields):

```
Router# show frame-relay multilink

Bundle: MFR0, state down, class C (threshold 2), no fragmentation
 ID: bundle
 Serial5/1, state up/up, ID: bundle1
 Serial5/3, state up/add-sent, ID: bundle3
```

Bundle Link: Example

The following is sample output from the **show frame-relay multilink** command when it is entered with the **serial** *number* keyword and argument pair (see Table 82 for descriptions of the fields). The example displays information about the specified bundle link:

```
Router# show frame-relay multilink serial 3/2

 Bundle links :
 Serial3/2, HW state : down, Protocol state :Down_idle, LID :Serial3/2
 Bundle interface = MFR0,  BID = MFR0
```

Detailed Bundle Links: Examples

The following is sample output from the **show frame-relay multilink** command when it is entered with the **serial** *number* keyword and argument pair and **detailed** keyword (see Table 82 for descriptions of the fields). The example shows a bundle link in the "idle" state:

```
Router# show frame-relay multilink serial 3 detailed

 Bundle links:

  Serial3, HW state = up, link state = Idle, LID = Serial3
  Bundle interface = MFR0,  BID = MFR0
    Cause code = none, Ack timer = 4, Hello timer = 10,
    Max retry count = 2, Current count = 0,
    Peer LID = Serial5/3, RTT = 0 ms
    Statistics:
    Add_link sent = 0, Add_link rcv'd = 10,
    Add_link ack sent = 0, Add_link ack rcv'd = 0,
    Add_link rej sent = 10, Add_link rej rcv'd = 0,
    Remove_link sent = 0, Remove_link rcv'd = 0,
    Remove_link_ack sent = 0, Remove_link_ack rcv'd = 0,
    Hello sent = 0, Hello rcv'd = 0,
    Hello_ack sent = 0, Hello_ack rcv'd = 0,
    outgoing pak dropped = 0, incoming pak dropped = 0
```

The following is sample output from the **show frame-relay multilink** command when it is entered with the **serial** *number* keyword and argument pair and **detailed** keyword (see Table 82 for descriptions of the fields). The example shows a bundle link in the "up" state:

```
Router# show frame-relay multilink serial 3 detailed

 Bundle links:

  Serial3, HW state = up, link state = Up, LID = Serial3
  Bundle interface = MFR0,  BID = MFR0
    Cause code = none, Ack timer = 4, Hello timer = 10,
    Max retry count = 2, Current count = 0,
    Peer LID = Serial5/3, RTT = 4 ms
    Statistics:
    Add_link sent = 1, Add_link rcv'd = 20,
    Add_link ack sent = 1, Add_link ack rcv'd = 1,
    Add_link rej sent = 19, Add_link rej rcv'd = 0,
    Remove_link sent = 0, Remove_link rcv'd = 0,
    Remove_link_ack sent = 0, Remove_link_ack rcv'd = 0,
    Hello sent = 0, Hello rcv'd = 1,
    Hello_ack sent = 1, Hello_ack rcv'd = 0,
    outgoing pak dropped = 0, incoming pak dropped = 0
```

Table 82 describes significant fields shown in the displays.

Table 82 show frame-relay multilink Field Descriptions

Field	Description
Bundle	Bundle interface.
State	Operational state of the bundle interface.
class	The bandwidth class criterion used to activate or deactivate a Frame Relay bundle. • Class A (single link)—The bundle activates when any bundle link is up and deactivates when all bundle links are down (default). • Class B (all links)—The bundle activates when all bundle links are up and deactivates when any bundle link is down. • Class C (threshold)—The bundle activates when the minimum configured number of bundle links (the threshold) is up and deactivates when the minimum number of configured bundle links fails to meet the threshold.
BID	Bundle identification.
Bundle links	Bundle links for which information is displayed.
HW state	Operational state of the physical link.
Protocol state	Operational state of the bundle link line protocol.
link state	Operational state of the bundle link.
LID	Bundle link identification.
Bundle interface	Bundle interface with which the bundle link is associated.

Table 82 show frame-relay multilink Field Descriptions (continued)

Field	Description
Cause code	Can be one of the following values: • ack timer expiry—Add link synchronization process is exhausted. • bundle link idle—Peer's bundle link is idle. This usually occurs when the peer's bundle interface is shut down. • inconsistent bundle—Peer already has this bundle associated with another bundle. • loopback detected—Local bundle link's physical line is looped back. • none—ADD_LINK and ADD_LINK_ACK messages were properly exchanged, and no cause code was recorded. • other—Indicates one of the following: a link identifier (LID) mismatch, an ID from the peer that is too long, or a failure to allocate ID memory. • unexpected Add_link—ADD_LINK message is received when the bundle link is already in the "up" state. This code might appear when the line protocol is being set up, but will disappear once the connection is stabilized.
Ack timer	Number of seconds for which the bundle link waits for a hello acknowledgment before resending a hello message or resending an ADD_LINK message used for initial synchronization.
Hello timer	Interval at which a bundle link sends out hello messages.
Max retry count	Maximum number of times that a bundle link will resend a hello message before receiving an acknowledgment or resending an ADD_LINK message.
Current count	Number of retries that have been attempted.
Peer LID	Bundle link identification name of the peer end of the link.
RTT	Round-trip time (in milliseconds) as measured by using the Timestamp Information Element in the HELLO and HELLO_ACK messages.
Statistics	Displays statistics for each bundle link.
Add_link sent	Number of Add_link messages sent. Add_link messages notify the peer endpoint that the local endpoint is ready to process frames.
Add_link rcv'd	Number of Add_link messages received.
Add_link ack sent	Number of Add_link acknowledgments sent. Add_link acknowledgments notify the peer endpoint that an Add_link message was received.
Add_link ack rcv'd	Number of Add_link acknowledgments received.
Add_link rej sent	Number of Add_link_reject messages sent.
Add_link rej rcv'd	Number of Add_link_reject messages received.

Table 82 show frame-relay multilink Field Descriptions (continued)

Field	Description
Remove_link sent	Number of Remove_link messages sent. Remove_link messages notify the peer that on the local end a bundle link is being removed from the bundle.
Remove_link rcv'd	Number of Remove_link messages received.
Remove_link_ack sent	Number of Remove_link acknowledgments sent. Remove_link acknowledgments notify the peer that a Remove_link message has been received.
Remove_link_ack rcv'd	Number of Remove_link acknowledgments received.
Hello sent	Number of hello messages sent. Hello messages notify the peer endpoint that the local endpoint remains in the "up" state.
Hello rcv'd	Number of hello messages received.
Hello_ack sent	Number of hello acknowledgments sent. Hello acknowledgments notify the peer that hello messages have been received.
Hello_ack rcv'd	Number of hello acknowledgments received.
outgoing pak dropped	Number of outgoing packets dropped.
incoming pak dropped	Number of incoming packets dropped.

Related Commands

Command	Description
debug frame-relay multilink	Displays debug messages for multilink Frame Relay bundles and bundle links.

show frame-relay pvc

To display statistics about Frame Relay permanent virtual circuits (PVCs), use the **show frame-relay pvc** command in privileged EXEC mode.

show frame-relay pvc [[**interface** *interface*] [*dlci*] [**64-bit**] | **summary** [**all**]]

Syntax Description

interface	(Optional) Specific interface for which PVC information will be displayed.
interface	(Optional) Interface number containing the data-link connection identifiers (DLCIs) for which you wish to display PVC information.
dlci	(Optional) A specific DLCI number used on the interface. Statistics for the specified PVC are displayed when a DLCI is also specified.
64-bit	(Optional) Displays 64-bit counter statistics.
summary	(Optional) Displays a summary of all PVCs on the system.
all	(Optional) Displays a summary of all PVCs on each interface.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.0(1)T	This command was modified to display statistics about virtual access interfaces used for PPP connections over Frame Relay.
12.0(3)XG	This command was modified to include the fragmentation type and size associated with a particular PVC when fragmentation is enabled on the PVC.
12.0(4)T	This command was modified to include the fragmentation type and size associated with a particular PVC when fragmentation is enabled on the PVC.
12.0(5)T	This command was modified to include information on the special voice queue that is created using the **queue** keyword of the **frame-relay voice bandwidth** command.
12.1(2)T	This command was modified to display the following information: • Details about the policy map attached to a specific PVC. • The priority configured for PVCs within Frame Relay PVC interface priority queueing. • Details about Frame Relay traffic shaping and policing on switched PVCs.
12.0(12)S	This command was modified to display reasons for packet drops and complete status information for switched NNI PVCs.
12.1(5)T	This command was modified to display the following information: • The number of packets in the post-hardware-compression queue. • The reasons for packet drops and complete status information for switched network-to-network PVCs.

Release	Modification
12.0(17)S	This command was modified to display the number of outgoing packets dropped and the number of outgoing bytes dropped because of QoS policy.
12.2 T	This command was modified to show that when payload compression is configured for a PVC, the throughput rate reported by the PVC is equal to the rate reported by the interface.
12.2(4)T	The **64-bit** keyword was added.
12.2(11)T	This command was modified to display the number of outgoing packets dropped and the number of outgoing bytes dropped because of QoS policy.
12.2(13)T	This command was modified to support display of Frame Relay PVC bundle information.
12.2(15)T	This command was modified to support display of Frame Relay voice-adaptive fragmentation information.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC, and the **summary** and **all** keywords were added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB, and support was added for hierarchical queueing framework (HQF).
12.4(9)T	The **summary** and **all** keywords were added, and support was added for hierarchical queueing framework (HQF).
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.
12.0(33)S	Support for IPv6 was added. This command was implemented on the Cisco 12000 series routers.

Usage Guidelines

Use this command to monitor the PPP link control protocol (LCP) state as being open with an up state or closed with a down state.

When “vofr” or “vofr cisco” has been configured on the PVC, and a voice bandwidth has been allocated to the class associated with this PVC, configured voice bandwidth and used voice bandwidth are also displayed.

Statistics Reporting

To obtain statistics about PVCs on all Frame Relay interfaces, use this command with no arguments.

To obtain statistics about a PVC that include policy-map configuration or the priority configured for that PVC, use this command with the *dlci* argument.

To display a summary of all PVCs on the system, use the **show frame-relay pvc** command with the **summary** keyword. To display a summary of all PVCs per interface, use the **summary all** keywords.

Per-VC counters are not incremented at all when either autonomous or silicon switching engine (SSE) switching is configured; therefore, PVC values will be inaccurate if either switching method is used.

You can change the period of time over which a set of data is used for computing load statistics. If you decrease the load interval, the average statistics are computed over a shorter period of time and are more responsive to bursts of traffic. To change the length of time for which a set of data is used to compute load statistics for a PVC, use the **load-interval** command in Frame-Relay DLCI configuration mode.

Traffic Shaping

Congestion control mechanisms are currently not supported on terminated PVCs nor on PVCs over ISDN. Where congestion control mechanisms are supported, the switch passes forward explicit congestion notification (FECN) bits, backward explicit congestion notification (BECN) bits, and discard eligible (DE) bits unchanged from entry points to exit points in the network.

Examples

The various displays in this section show sample output for a variety of PVCs. Some of the PVCs carry data only; some carry a combination of voice and data. This section contains the following examples:

Summary of Frame Relay PVCs: Example

The following example shows sample output of the **show frame-relay pvc** command with the **summary** keyword. The **summary** keyword displays all PVCs on the system.

```
Router# show frame-relay pvc summary

Frame-Relay VC Summary

                Active      Inactive      Deleted       Static
  Local            0            12            0            0
  Switched         0             0            0            0
  Unused           0             0            0            0
```

The following example shows sample output for the **show frame-relay pvc** command with the **summary** and **all** keywords. The **summary** and **all** keywords display all PVCs per interface.

```
Router# show frame-relay pvc summary all

VC Summary for interface Serial3/0 (Frame Relay DTE)
```

```
              Active     Inactive      Deleted       Static
  Local          0            7            0            0
  Switched       0            0            0            0
  Unused         0            0            0            0

VC Summary for interface Serial3/1 (Frame Relay DTE)

              Active     Inactive      Deleted       Static
  Local          0            5            0            0
  Switched       0            0            0            0
  Unused         0            0            0            0
```

Frame Relay Generic Configuration: Example

The following sample output shows a generic Frame Relay configuration on DLCI 100:

```
Router# show frame-relay pvc 100

PVC Statistics for interface Serial4/0/1:0 (Frame Relay DTE)

DLCI = 100, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE (EEK UP), INTERFACE = Serial4/0/1:0.1

  input pkts 4360          output pkts 4361         in bytes 146364
  out bytes 130252         dropped pkts 3735        in pkts dropped 0
  out pkts dropped 3735             out bytes dropped 1919790
  late-dropped out pkts 3735        late-dropped out bytes 1919790
  in FECN pkts 0           in BECN pkts 0           out FECN pkts 0
  out BECN pkts 0          in DE pkts 0             out DE pkts 0
  out bcast pkts 337       out bcast bytes 102084
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  pvc create time 05:34:06, last time pvc status changed 05:33:38
```

Frame Relay Voice-Adaptive Fragmentation: Example

The following sample output indicates that Frame Relay voice-adaptive fragmentation is active on DLCI 202 and there are 29 seconds left on the deactivation timer. If no voice packets are detected in the next 29 seconds, Frame Relay voice-adaptive fragmentation will become inactive.

```
Router# show frame-relay pvc 202

PVC Statistics for interface Serial3/1 (Frame Relay DTE)

DLCI = 202, DLCI USAGE = LOCAL, PVC STATUS = STATIC, INTERFACE = Serial3/1.2

  input pkts 0             output pkts 479          in bytes 0
  out bytes 51226          dropped pkts 0           in pkts dropped 0
  out pkts dropped 0                out bytes dropped 0
  in FECN pkts 0           in BECN pkts 0           out FECN pkts 0
  out BECN pkts 0          in DE pkts 0             out DE pkts 0
  out bcast pkts 0         out bcast bytes 0
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 5000 bits/sec, 5 packets/sec
  pvc create time 00:23:36, last time pvc status changed 00:23:31
  fragment type end-to-end fragment size 80 adaptive active, time left 29 secs
```

Frame Relay PVC Bundle: Example

The following sample output indicates that PVC 202 is a member of VC bundle MAIN-1-static:

```
Router# show frame-relay pvc 202

PVC Statistics for interface Serial1/4 (Frame Relay DTE)

DLCI = 202, DLCI USAGE = LOCAL, PVC STATUS = STATIC, INTERFACE = Serial1/4
```

```
  input pkts 0             output pkts 45           in bytes 0
  out bytes 45000          dropped pkts 0           in FECN pkts 0
  in BECN pkts 0           out FECN pkts 0          out BECN pkts 0
  in DE pkts 0             out DE pkts 0
  out bcast pkts 0         out bcast bytes 0
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 2000 bits/sec, 2 packets/sec
  pvc create time 00:01:25, last time pvc status changed 00:01:11
  VC-Bundle MAIN-1-static
```

Frame Relay 64-Bit Counter: Example

The following sample output displays the Frame Relay 64-bit counters:

```
Router# show frame-relay pvc 35 64-bit

DLCI = 35, INTERFACE = Serial0/0
  input pkts 0                       output pkts 0
  in bytes 0                         out bytes 0
```

Frame Relay Fragmentation and Hardware Compression: Example

The following is sample output for the **show frame-relay pvc** command for a PVC configured with Cisco-proprietary fragmentation and hardware compression:

```
Router# show frame-relay pvc 110

PVC Statistics for interface Serial0/0 (Frame Relay DTE)

DLCI = 110, DLCI USAGE = LOCAL, PVC STATUS = STATIC, INTERFACE = Serial0/0

  input pkts 409           output pkts 409          in bytes 3752
  out bytes 4560           dropped pkts 1           in FECN pkts 0
  in BECN pkts 0           out FECN pkts 0          out BECN pkts 0
  in DE pkts 0             out DE pkts 0
  out bcast pkts 0          out bcast bytes 0
  pvc create time 3d00h, last time pvc status changed 2d22h
  Service type VoFR-cisco
   Voice Queueing Stats: 0/100/0 (size/max/dropped)
  Post h/w compression queue: 0
  Current fair queue configuration:
   Discard     Dynamic      Reserved
   threshold   queue count  queue count
   64          16           2
  Output queue size 0/max total 600/drops 0
  configured voice bandwidth 16000, used voice bandwidth 0
  fragment type VoFR-cisco         fragment size 100
  cir 64000     bc   640       be 0         limit 80     interval 10
  mincir 32000     byte increment 80    BECN response no
  frags 428       bytes 4810      frags delayed 24        bytes delayed 770
  shaping inactive
  traffic shaping drops 0
  ip rtp priority parameters 16000 32000 20000
```

Switched PVC: Example

The following is sample output from the **show frame-relay pvc** command for a switched Frame Relay PVC. This output displays detailed information about Network-to-Network Interface (NNI) status and why packets were dropped from switched PVCs.

```
Router# show frame-relay pvc

 PVC Statistics for interface Serial2/2 (Frame Relay NNI)
```

```
 DLCI = 16, DLCI USAGE = SWITCHED, PVC STATUS = INACTIVE, INTERFACE = Serial2/2
 LOCAL PVC STATUS = INACTIVE, NNI PVC STATUS = INACTIVE

   input pkts 0             output pkts 0            in bytes 0
   out bytes 0              dropped pkts 0           in FECN pkts 0
   in BECN pkts 0           out FECN pkts 0          out BECN pkts 0
   in DE pkts 0             out DE pkts 0
   out bcast pkts 0         out bcast bytes 0
   switched pkts0
   Detailed packet drop counters:
   no out intf 0            out intf down 0          no out PVC 0
   in PVC down 0            out PVC down 0           pkt too big 0
   shaping Q full 0         pkt above DE 0           policing drop 0
   pvc create time 00:00:07, last time pvc status changed 00:00:07
```

Frame Relay Congestion Management on a Switched PVC: Example

The following is sample output from the **show frame-relay pvc** command that shows the statistics for a switched PVC on which Frame Relay congestion management is configured:

```
Router# show frame-relay pvc 200

PVC Statistics for interface Serial3/0 (Frame Relay DTE)

DLCI = 200, DLCI USAGE = SWITCHED, PVC STATUS = ACTIVE, INTERFACE = Serial3/0

  input pkts 341           output pkts 390          in bytes 341000
  out bytes 390000         dropped pkts 0           in FECN pkts 0
  in BECN pkts 0           out FECN pkts 0          out BECN pkts 0
  in DE pkts 0             out DE pkts 390
  out bcast pkts 0          out bcast bytes 0            Num Pkts Switched 341

  pvc create time 00:10:35, last time pvc status changed 00:10:06
  Congestion DE threshold 50
  shaping active
  cir 56000     bc 7000      be 0         byte limit 875    interval 125
  mincir 28000     byte increment 875   BECN response no
  pkts 346       bytes 346000    pkts delayed 339       bytes delayed 339000
  traffic shaping drops 0
  Queueing strategy:fifo
  Output queue 48/100, 0 drop, 339 dequeued
```

Frame Relay Policing on a Switched PVC: Example

The following is sample output from the **show frame-relay pvc** command that shows the statistics for a switched PVC on which Frame Relay policing is configured:

```
Router# show frame-relay pvc 100

PVC Statistics for interface Serial1/0 (Frame Relay DCE)

DLCI = 100, DLCI USAGE = SWITCHED, PVC STATUS = ACTIVE, INTERFACE = Serial1/0

  input pkts 1260          output pkts 0            in bytes 1260000
  out bytes 0              dropped pkts 0           in FECN pkts 0
  in BECN pkts 0           out FECN pkts 0          out BECN pkts 0
  in DE pkts 0             out DE pkts 0
  out bcast pkts 0          out bcast bytes 0            Num Pkts Switched 1260

  pvc create time 00:03:57, last time pvc status changed 00:03:19
  policing enabled, 180 pkts marked DE
  policing Bc  6000        policing Be  6000        policing Tc  125 (msec)
  in Bc pkts   1080        in Be pkts   180         in xs pkts   0
  in Bc bytes  1080000     in Be bytes  180000      in xs bytes  0
```

Frame Relay PVC Priority Queueing: Example

The following is sample output for a PVC that has been assigned high priority:

```
Router# show frame-relay pvc 100

PVC Statistics for interface Serial0 (Frame Relay DTE)

DLCI = 100, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0

  input pkts 0             output pkts 0            in bytes 0
  out bytes 0              dropped pkts 0           in FECN pkts 0
  in BECN pkts 0           out FECN pkts 0          out BECN pkts 0
  in DE pkts 0             out DE pkts 0
  out bcast pkts 0          out bcast bytes 0
  pvc create time 00:00:59, last time pvc status changed 00:00:33
  priority high
```

Low Latency Queueing for Frame Relay: Example

The following is sample output from the **show frame-relay pvc** command for a PVC shaped to a 64000 bps committed information rate (CIR) with fragmentation. A policy map is attached to the PVC and is configured with a priority class for voice, two data classes for IP precedence traffic, and a default class for best-effort traffic. Weighted Random Early Detection (WRED) is used as the drop policy on one of the data classes.

```
Router# show frame-relay pvc 100

PVC Statistics for interface Serial1/0 (Frame Relay DTE)

DLCI = 100, DLCI USAGE = LOCAL, PVC STATUS = INACTIVE, INTERFACE = Serial1/0.1

  input pkts 0             output pkts 0            in bytes 0
  out bytes 0              dropped pkts 0           in FECN pkts 0
  in BECN pkts 0           out FECN pkts 0          out BECN pkts 0
  in DE pkts 0             out DE pkts 0
  out bcast pkts 0          out bcast bytes 0
  pvc create time 00:00:42, last time pvc status changed 00:00:42
  service policy mypolicy
 Class voice
  Weighted Fair Queueing
      Strict Priority
      Output Queue: Conversation 72
        Bandwidth 16 (kbps) Packets Matched 0
        (pkts discards/bytes discards) 0/0
 Class immediate-data
  Weighted Fair Queueing
      Output Queue: Conversation 73
        Bandwidth 60 (%) Packets Matched 0
        (pkts discards/bytes discards/tail drops) 0/0/0
        mean queue depth: 0
        drops: class  random   tail     min-th   max-th   mark-prob
               0      0        0        64       128      1/10
               1      0        0        71       128      1/10
               2      0        0        78       128      1/10
               3      0        0        85       128      1/10
               4      0        0        92       128      1/10
               5      0        0        99       128      1/10
               6      0        0        106      128      1/10
               7      0        0        113      128      1/10
               rsvp   0        0        120      128      1/10
 Class priority-data
  Weighted Fair Queueing
      Output Queue: Conversation 74
```

```
       Bandwidth 40 (%) Packets Matched 0 Max Threshold 64 (packets)
       (pkts discards/bytes discards/tail drops) 0/0/0
 Class class-default
  Weighted Fair Queueing
      Flow Based Fair Queueing
      Maximum Number of Hashed Queues 64  Max Threshold 20 (packets)
  Output queue size 0/max total 600/drops 0
  fragment type end-to-end         fragment size 50
  cir 64000     bc   640       be 0         limit 80     interval 10
  mincir 64000     byte increment 80    BECN response no
  frags 0         bytes 0         frags delayed 0         bytes delayed 0
  shaping inactive
  traffic shaping drops 0
```

PPP over Frame Relay: Example

The following is sample output from the **show frame-relay pvc** command that shows the PVC statistics for serial interface 5 (slot 1 and DLCI 55 are up) during a PPP session over Frame Relay:

```
Router# show frame-relay pvc 55

PVC Statistics for interface Serial5/1 (Frame Relay DTE)
DLCI = 55, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial5/1.1
     input pkts 9             output pkts 16           in bytes 154
     out bytes 338            dropped pkts 6           in FECN pkts 0
     in BECN pkts 0           out FECN pkts 0          out BECN pkts 0
     in DE pkts 0             out DE pkts 0
     out bcast pkts 0         out bcast bytes 0
     pvc create time 00:35:11, last time pvc status changed 00:00:22
     Bound to Virtual-Access1 (up, cloned from Virtual-Template5)
```

Voice over Frame Relay: Example

The following is sample output from the **show frame-relay pvc** command for a PVC carrying Voice over Frame Relay (VoFR) traffic configured via the **vofr cisco** command. The **frame-relay voice bandwidth** command has been configured on the class associated with this PVC, as has fragmentation. The fragmentation type employed is proprietary to Cisco.

A sample configuration for this situation is shown first, followed by the output for the **show frame-relay pvc** command.

```
interface serial 0
 encapsulation frame-relay
 frame-relay traffic-shaping
 frame-relay interface-dlci 108
  vofr cisco
  class vofr-class
map-class frame-relay vofr-class
 frame-relay fragment 100
 frame-relay fair-queue
 frame-relay cir 64000
 frame-relay voice bandwidth 25000

Router# show frame-relay pvc 108

PVC Statistics for interface Serial0 (Frame Relay DTE)
DLCI = 108, DLCI USAGE = LOCAL, PVC STATUS = STATIC, INTERFACE = Serial0
  input pkts 1260          output pkts 1271         in bytes 95671
  out bytes 98604          dropped pkts 0           in FECN pkts 0
  in BECN pkts 0           out FECN pkts 0          out BECN pkts 0
  in DE pkts 0             out DE pkts 0
  out bcast pkts 1271       out bcast bytes 98604
  pvc create time 09:43:17, last time pvc status changed 09:43:17
  Service type VoFR-cisco
```

```
  configured voice bandwidth 25000, used voice bandwidth 0
  voice reserved queues 24, 25
  fragment type VoFR-cisco         fragment size 100
  cir 64000     bc 64000     be 0         limit 1000   interval 125
  mincir 32000     byte increment 1000  BECN response no
  pkts 2592      bytes 205140    pkts delayed 1296      bytes delayed 102570
  shaping inactive
  shaping drops 0
  Current fair queue configuration:
   Discard     Dynamic      Reserved
   threshold   queue count  queue count
    64          16           2
  Output queue size 0/max total 600/drops 0
```

FRF.12 Fragmentation: Example

The following is sample output from the **show frame-relay pvc** command for an application employing pure FRF.12 fragmentation. A sample configuration for this situation is shown first, followed by the output for the **show frame-relay pvc** command.

```
interface serial 0
 encapsulation frame-relay
 frame-relay traffic-shaping
 frame-relay interface-dlci 110
  class frag
map-class frame-relay frag
 frame-relay fragment 100
 frame-relay fair-queue
 frame-relay cir 64000

Router# show frame-relay pvc 110

PVC Statistics for interface Serial0 (Frame Relay DTE)
DLCI = 110, DLCI USAGE = LOCAL, PVC STATUS = STATIC, INTERFACE = Serial0
  input pkts 0             output pkts 243          in bytes 0
  out bytes 7290           dropped pkts 0           in FECN pkts 0
  in BECN pkts 0           out FECN pkts 0          out BECN pkts 0
  in DE pkts 0             out DE pkts 0
  out bcast pkts 243        out bcast bytes 7290
  pvc create time 04:03:17, last time pvc status changed 04:03:18
  fragment type end-to-end         fragment size 100
  cir 64000     bc 64000     be 0         limit 1000   interval 125
  mincir 32000     byte increment 1000  BECN response no
  pkts 486       bytes 14580     pkts delayed 243       bytes delayed 7290
  shaping inactive
  shaping drops 0
  Current fair queue configuration:
   Discard     Dynamic      Reserved
   threshold   queue count  queue count
   64          16           2
  Output queue size 0/max total 600/drops 0
```

Note that when voice is not configured, voice bandwidth output is not displayed.

Multipoint Subinterfaces Transporting Data: Example

The following is sample output from the **show frame-relay pvc** command for multipoint subinterfaces carrying data only. The output displays both the subinterface number and the DLCI. This display is the same whether the PVC is configured for static or dynamic addressing. Note that neither fragmentation nor voice is configured on this PVC.

```
Router# show frame-relay pvc

DLCI = 300, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0.103
input pkts 10  output pkts 7  in bytes 6222
out bytes 6034  dropped pkts 0  in FECN pkts 0
in BECN pkts 0  out FECN pkts 0  out BECN pkts 0
in DE pkts 0  out DE pkts 0
outbcast pkts 0  outbcast bytes 0
pvc create time 0:13:11  last time pvc status changed 0:11:46
DLCI = 400, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0.104
input pkts 20  output pkts 8  in bytes 5624
out bytes 5222  dropped pkts 0  in FECN pkts 0
in BECN pkts 0  out FECN pkts 0  out BECN pkts 0
in DE pkts 0  out DE pkts 0
outbcast pkts 0  outbcast bytes 0
pvc create time 0:03:57  last time pvc status changed 0:03:48
```

PVC Shaping When HQF is Enabled: Example

The following is sample output from the **show frame-relay pvc** command for a PVC when HQF is enabled:

```
Router# show frame-relay pvc 16

PVC Statistics for interface Serial4/1 (Frame Relay DTE)

DLCI = 16, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial4/1

  input pkts 1             output pkts 1            in bytes 34
  out bytes 34             dropped pkts 0           in pkts dropped 0
  out pkts dropped 0                out bytes dropped 0
  in FECN pkts 0           in BECN pkts 0           out FECN pkts 0
  out BECN pkts 0          in DE pkts 0             out DE pkts 0
  out bcast pkts 1         out bcast bytes 34
  pvc create time 00:09:07, last time pvc status changed 00:09:07
  shaping inactive
```

PVC Transporting Voice and Data: Example

The following is sample output from the **show frame-relay pvc** command for a PVC carrying voice and data traffic, with a special queue specifically for voice traffic created using the **frame-relay voice bandwidth** command **queue** keyword:

```
Router# show frame-relay pvc interface serial 1 45

 PVC Statistics for interface Serial1 (Frame Relay DTE)

 DLCI = 45, DLCI USAGE = LOCAL, PVC STATUS = STATIC, INTERFACE = Serial1

   input pkts 85            output pkts 289          in bytes 1730
   out bytes 6580           dropped pkts 11          in FECN pkts 0
   in BECN pkts 0           out FECN pkts 0          out BECN pkts 0
   in DE pkts 0             out DE pkts 0
   out bcast pkts 0          out bcast bytes 0
   pvc create time 00:02:09, last time pvc status changed 00:02:09
   Service type VoFR
   configured voice bandwidth 25000, used voice bandwidth 22000
   fragment type VoFR         fragment size 100
   cir 20000     bc   1000      be 0         limit 125    interval 50
   mincir 20000     byte increment 125   BECN response no
   fragments 290       bytes 6613      fragments delayed 1         bytes delayed 33
   shaping inactive
   traffic shaping drops 0
    Voice Queueing Stats: 0/100/0 (size/max/dropped)
```

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Current fair queue configuration:
 Discard     Dynamic      Reserved
 threshold   queue count  queue count
 64          16           2
Output queue size 0/max total 600/drops 0
```

Table 83 describes the significant fields shown in the displays.

Table 83 show frame-relay pvc Field Descriptions

Field	Description
DLCI	One of the DLCI numbers for the PVC.
DLCI USAGE	Lists SWITCHED when the router or access server is used as a switch, or LOCAL when the router or access server is used as a DTE device.
PVC STATUS	Status of the PVC: ACTIVE, INACTIVE, or DELETED.
INTERFACE	Specific subinterface associated with this DLCI.
LOCAL PVC STATUS[1]	Status of PVC configured locally on the NNI interface.
NNI PVC STATUS[1]	Status of PVC learned over the NNI link.
input pkts	Number of packets received on this PVC.
output pkts	Number of packets sent on this PVC.
in bytes	Number of bytes received on this PVC.
out bytes	Number of bytes sent on this PVC.
dropped pkts	Number of incoming and outgoing packets dropped by the router at the Frame Relay level.
in pkts dropped	Number of incoming packets dropped. Incoming packets may be dropped for a number of reasons, including the following: • Inactive PVC • Policing • Packets received above DE discard level • Dropped fragments • Memory allocation failures • Configuration problems
out pkts dropped	Number of outgoing packets dropped, including shaping drops and late drops.
out bytes dropped	Number of outgoing bytes dropped.
late-dropped out pkts	Number of outgoing packets dropped because of QoS policy (such as with VC queuing or Frame Relay traffic shaping). This field is not displayed when the value is zero.
late-dropped out bytes	Number of outgoing bytes dropped because of QoS policy (such with as VC queuing or Frame Relay traffic shaping). This field is not displayed when the value is zero.
in FECN pkts	Number of packets received with the FECN bit set.
in BECN pkts	Number of packets received with the BECN bit set.

Table 83 show frame-relay pvc Field Descriptions (continued)

Field	Description
out FECN pkts	Number of packets sent with the FECN bit set.
out BECN pkts	Number of packets sent with the BECN bit set.
in DE pkts	Number of DE packets received.
out DE pkts	Number of DE packets sent.
out bcast pkts	Number of output broadcast packets.
out bcast bytes	Number of output broadcast bytes.
switched pkts	Number of switched packets.
no out intf[2]	Number of packets dropped because there is no output interface.
out intf down[2]	Number of packets dropped because the output interface is down.
no out PVC[2]	Number of packets dropped because the outgoing PVC is not configured.
in PVC down[2]	Number of packets dropped because the incoming PVC is inactive.
out PVC down[2]	Number of packets dropped because the outgoing PVC is inactive.
pkt too big[2]	Number of packets dropped because the packet size is greater than media MTU[3].
shaping Q full[2]	Number of packets dropped because the Frame Relay traffic-shaping queue is full.
pkt above DE[2]	Number of packets dropped because they are above the DE level when Frame Relay congestion management is enabled.
policing drop[2]	Number of packets dropped because of Frame Relay traffic policing.
pvc create time	Time at which the PVC was created.
last time pvc status changed	Time at which the PVC changed status.
VC-Bundle	PVC bundle of which the PVC is a member.
priority	Priority assigned to the PVC.
pkts marked DE	Number of packets marked DE because they exceeded the Bc.
policing Bc	Committed burst size.
policing Be	Excess burst size.
policing Tc	Measurement interval for counting Bc and Be.
in Bc pkts	Number of packets received within the committed burst.
in Be pkts	Number of packets received within the excess burst.
in xs pkts	Number of packets dropped because they exceeded the combined burst.
in Bc bytes	Number of bytes received within the committed burst.
in Be bytes	Number of bytes received within the excess burst.
in xs bytes	Number of bytes dropped because they exceeded the combined burst.
Congestion DE threshold	PVC queue percentage at which packets with the DE bit are dropped.
Congestion ECN threshold	PVC queue percentage at which packets are set with the BECN and FECN bits.

Table 83 show frame-relay pvc Field Descriptions (continued)

Field	Description
Service type	Type of service performed by this PVC. Can be VoFR or VoFR-cisco.
Post h/w compression queue	Number of packets in the post-hardware-compression queue when hardware compression and Frame Relay fragmentation are configured.
configured voice bandwidth	Amount of bandwidth in bits per second (bps) reserved for voice traffic on this PVC.
used voice bandwidth	Amount of bandwidth in bps currently being used for voice traffic.
service policy	Name of the output service policy applied to the VC.
Class	Class of traffic being displayed. Output is displayed for each configured class in the policy.
Output Queue	The WFQ[4] conversation to which this class of traffic is allocated.
Bandwidth	Bandwidth in kbps or percentage configured for this class.
Packets Matched	Number of packets that matched this class.
Max Threshold	Maximum queue size for this class when WRED is not used.
pkts discards	Number of packets discarded for this class.
bytes discards	Number of bytes discarded for this class.
tail drops	Number of packets discarded for this class because the queue was full.
mean queue depth	Average queue depth, based on the actual queue depth on the interface and the exponential weighting constant. It is a moving average. The minimum and maximum thresholds are compared against this value to determine drop decisions.
drops:	WRED parameters.
class	IP precedence value.
random	Number of packets randomly dropped when the mean queue depth is between the minimum threshold value and the maximum threshold value for the specified IP precedence value.
tail	Number of packets dropped when the mean queue depth is greater than the maximum threshold value for the specified IP precedence value.
min-th	Minimum WRED threshold in number of packets.
max-th	Maximum WRED threshold in number of packets.
mark-prob	Fraction of packets dropped when the average queue depth is at the maximum threshold.
Maximum Number of Hashed Queues	(Applies to class default only) Number of queues available for unclassified flows.
fragment type	Type of fragmentation configured for this PVC. Possible types are as follows: • end-to-end—Fragmented packets contain the standard FRF.12 header • VoFR—Fragmented packets contain the FRF.11 Annex C header • VoFR-cisco—Fragmented packets contain the Cisco proprietary header
fragment size	Size of the fragment payload in bytes.

Table 83 show frame-relay pvc Field Descriptions (continued)

Field	Description
adaptive active/inactive	Indicates whether Frame Relay voice-adaptive fragmentation is active or inactive.
time left	Number of seconds left on the Frame Relay voice-adaptive fragmentation deactivation timer. When this timer expires, Frame Relay fragmentation turns off.
cir	Current CIR in bps.
bc	Current committed burst (Bc) size, in bits.
be	Current excess burst (Be) size, in bits.
limit	Maximum number of bytes sent per internal interval (excess plus sustained).
interval	Interval being used internally (may be smaller than the interval derived from Bc/CIR; this happens when the router determines that traffic flow will be more stable with a smaller configured interval).
mincir	Minimum CIR for the PVC.
byte increment	Number of bytes that will be sustained per internal interval.
BECN response	Indication that Frame Relay has BECN adaptation configured.
pkts	Number of packets associated with this PVC that have gone through the traffic-shaping system.
frags	Total number of fragments (and unfragmented packets that are too small to be fragmented) shaped on this VC.
bytes	Number of bytes associated with this PVC that have gone through the traffic-shaping system.
pkts delayed	Number of packets associated with this PVC that have been delayed by the traffic-shaping system.
frags delayed	Number of fragments (and unfragmented packets that are too small to be fragmented) delayed in the shaping queue before being sent.
bytes delayed	Number of bytes associated with this PVC that have been delayed by the traffic-shaping system.
shaping	Indication that shaping will be active for all PVCs that are fragmenting data; otherwise, shaping will be active if the traffic being sent exceeds the CIR for this circuit.
shaping drops	Number of packets dropped by the traffic-shaping process.
Queueing strategy	Per-VC queueing strategy.
Output queue 48/100 0 drop 300 dequeued	State of the per-VC queue. • Number of packets enqueued/size of the queue • Number of packets dropped • Number of packets dequeued
Voice Queueing Stats	Statistics showing the size of packets, the maximum number of packets, and the number of packets dropped in the special voice queue created using the **frame-relay voice bandwidth** command **queue** keyword.

Table 83 show frame-relay pvc Field Descriptions (continued)

Field	Description
Discard threshold	Maximum number of packets that can be stored in each packet queue. Additional packets received after a queue is full will be discarded.
Dynamic queue count	Number of packet queues reserved for best-effort traffic.
Reserved queue count	Number of packet queues reserved for voice traffic.
Output queue size	Size in bytes of each output queue.
max total	Maximum number of packets of all types that can be queued in all queues.
drops	Number of frames dropped by all output queues.

1. The LOCAL PVC STATUS and NNI PVC STATUS fields are displayed only for PVCs configured on Frame Relay NNI interface types. These fields are not displayed if the PVC is configured on DCE or DTE interface types.
2. The detailed packet drop fields are displayed for switched Frame Relay PVCs only. These fields are not displayed for terminated PVCs.
3. MTU = maximum transmission unit.
4. WFQ = weighted fair queueing.

Related Commands

Command	Description
frame-relay accounting adjust	Enables byte count adjustment at the PVC level so that the number of bytes sent and received at the PVC corresponds to the actual number of bytes sent and received on the physical interface.
frame-relay interface-queue priority	Enables FR PIPQ on a Frame Relay interface and assigns priority to a PVC within a Frame Relay map class.
frame-relay pvc	Configures Frame Relay PVCs for FRF.8 Frame Relay-ATM Service Interworking.
service-policy	Attaches a policy map to an input interface or VC or an output interface or VC.
show dial-peer voice	Displays configuration information and call statistics for dial peers.
show frame-relay fragment	Displays Frame Relay fragmentation details.
show frame-relay map	Displays the current Frame Relay map entries and information about the connections
show frame-relay vc-bundle	Displays attributes and other information about a Frame Relay PVC bundle.

show glbp

To display Gateway Load Balancing Protocol (GLBP) information, use the **show glbp** command in privileged EXEC mode.

show glbp [**capability** [*interface-type interface-number*]] | [[*interface-type interface-number* [*group-number*] [*state*] [**brief**] [**detail**] [**client-cache** [[**age** *number*] [**forwarder** *number*]] | [**mac-address** *address*] | [**summary**]]]

Syntax Description

interface-type interface-number	(Optional) Interface type and number for which output is displayed.
group-number	(Optional) GLBP group number in the range from 0 to 1023.
state	(Optional) State of the GLBP router, one of the following: **active**, **disabled**, **init**, **listen**, and **standby**.
brief	(Optional) Summarizes each virtual gateway or virtual forwarder with a single line of output.
detail	(Optional) Displays all the status of the GLBP router in detailed format. The available status are: **active**, **disabled**, **init**, **listen**, **speak**, and **standby**.
capability	(Optional) Displays the GLBP capability interfaces.
client-cache	(Optional) Displays the GLBP client cache.
age *number*	(Optional) Displays the client-cache age in the range from 0 to 1440.
forwarder *number*	(Optional) Displays the client forwarder in the range from 1 to 4.
mac-address *address*	(Optional) Displays the mac-address of the client.
summary	(Optional) Displays the summary of the GLBP client caches.

Command Modes

Privileged EXEC (#)

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. The **client-cache** keyword was added.
12.3(2)T	The output was enhanced to display information about Message Digest 5 (MD5) authentication.
12.3(7)T	The output was enhanced to display information about assigned redundancy names to specified groups.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was enhanced to display information about GLBP support of Stateful Switchover (SSO) mode.
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.

Release	Modification
12.4(15)T	This command was modified. The **client-cache** keyword was added.
12.4(24)T	This command was modified. The **detail** keyword was added. The output was modified to hide configured passwords when MD5 key-string or text authentication is configured.
12.2(33)SXI1	This command was modified. The **client-cache** keyword was added. The output was modified to hide configured passwords when MD5 key-string or text authentication is configured.
12.2(33)SRE	The output was modified to hide configured passwords when MD5 key-string or text authentication is configured.

Usage Guidelines

Use the **show glbp** command to display information about GLBP groups on a router. The **brief** keyword displays a single line of information about each virtual gateway or virtual forwarder. The **client-cache** keyword displays the client cache details and the **capability** keyword displays all GLBP-capable interfaces.

Examples

The following is sample output from the **show glbp** command:

```
Router# show glbp

FastEthernet0/0 - Group 10
  State is Active
    2 state changes, last state change 23:50:33
  Virtual IP address is 10.21.8.10
  Hello time 5 sec, hold time 18 sec
    Next hello sent in 4.300 secs
  Redirect time 600 sec, forwarder time-out 7200 sec
  Authentication MD5, key-string
  Preemption enabled, min delay 60 sec
  Active is local
  Standby is unknown
  Priority 254 (configured)
  Weighting 105 (configured 110), thresholds: lower 95, upper 105
    Track object 2 state Down decrement 5
  Load balancing: host-dependent
  There is 1 forwarder (1 active)
  Forwarder 1
    State is Active
      1 state change, last state change 23:50:15
    MAC address is 0007.b400.0101 (default)
    Owner ID is 0005.0050.6c08
    Redirection enabled
    Preemption enabled, min delay 60 sec
    Active is local, weighting 105
```

The following is sample output from the **show glbp** command with the **brief** keyword specified:

```
Router# show glbp brief

Interface   Grp  Fwd Pri State    Address         Active router   Standby router
Fa0/0       10   -   254 Active   10.21.8.10       local           unknown
Fa0/0       10   1   7   Active   0007.b400.0101   local           -
```

The following is sample output from the **show glbp** command that displays GLBP group 10:

```
Router# show glbp 10

FastEthernet0/0 - Group 10
  State is Active
    2 state changes, last state change 23:50:33
  Virtual IP address is 10.21.8.10
  Hello time 5 sec, hold time 18 sec
    Next hello sent in 4.300 secs
  Redirect time 600 sec, forwarder time-out 7200 sec
  Authentication MD5, key-string
  Preemption enabled, min delay 60 sec
  Active is local
  Standby is unknown
  Priority 254 (configured)
  Weighting 105 (configured 110), thresholds: lower 95, upper 105
    Track object 2 state Down decrement 5
  Load balancing: host-dependent
  There is 1 forwarder (1 active)
  Forwarder 1
    State is Active
      1 state change, last state change 23:50:15
    MAC address is 0007.b400.0101 (default)
    Owner ID is 0005.0050.6c08
    Redirection enabled
    Preemption enabled, min delay 60 sec
    Active is local, weighting 105
```

The following output shows that the redundancy name has been assigned to the “glbp1” group:

```
Router# show glbp ethernet0/1 1

Ethernet0/1 - Group 1
 State is Listen
   64 state changes, last state change 00:00:54
 Virtual IP address is 10.1.0.7
 Hello time 50 msec, hold time 200 msec
   Next hello sent in 0.030 secs
 Redirect time 600 sec, forwarder time-out 14400 sec
  Authentication text, string "authword"
 Preemption enabled, min delay 0 sec
 Active is 10.1.0.2, priority 105 (expires in 0.184 sec)
 Standby is 10.1.0.3, priority 100 (expires in 0.176 sec)
 Priority 96 (configured)
 Weighting 100 (configured 100), thresholds: lower 95, upper 100
   Track object 1 state Up decrement 10
 Load balancing: round-robin
 IP redundancy name is "glbp1"
  Group members:
   0004.4d83.4801 (10.0.0.0)
   0010.7b5a.fa41 (10.0.0.1)
   00d0.bbd3.bc21 (10.0.0.2) local
```

The following output shows GLBP support for SSO mode on an active RP:

```
Router# show glbp

Ethernet0/0 - Group 1
State is Standby
1 state change, last state change 00:00:20
Virtual IP address is 172.24.1.254
Hello time 3 sec, hold time 10 sec
Next hello sent in 0.232 secs
Redirect time 600 sec, forwarder time-out 14400 sec
Preemption disabled
```

```
Active is 172.24.1.2, priority 100 (expires in 7.472 sec)
Standby is local
Priority 100 (default)
Weighting 100 (default 100), thresholds: lower 1, upper 100
Load balancing: round-robin
Group members:
aabb.cc00.0100 (172.24.1.1) local
aabb.cc00.0200 (172.24.1.2)
There are 2 forwarders (1 active)
Forwarder 1
State is Listen
MAC address is 0007.b400.0101 (learnt)
Owner ID is aabb.cc00.0200
Time to live: 14397.472 sec (maximum 14400 sec)
Preemption enabled, min delay 30 sec
Active is 172.24.1.2 (primary), weighting 100 (expires in 9.540 sec)
Forwarder 2
State is Active
1 state change, last state change 00:00:28
MAC address is 0007.b400.0102 (default)
Owner ID is aabb.cc00.0100
Preemption enabled, min delay 30 sec
Active is local, weighting 100
```

The following output shows GLBP support for SSO mode on a standby RP:

```
RouterRP-standby# show glbp

Ethernet0/0 - Group 1
State is Init (standby RP, peer state is Standby)
Virtual IP address is 172.24.1.254
Hello time 3 sec, hold time 10 sec
Redirect time 600 sec, forwarder time-out 14400 sec
Preemption disabled
Active is unknown
Standby is unknown
Priority 100 (default)
Weighting 100 (default 100), thresholds: lower 1, upper 100
Load balancing: round-robin
Group members:
aabb.cc00.0100 (172.24.1.1) local
aabb.cc00.0200 (172.24.1.2)
There are 2 forwarders (0 active)
Forwarder 1
State is Init (standby RP, peer state is Listen)
MAC address is 0007.b400.0101 (learnt)
Owner ID is aabb.cc00.0200
Preemption enabled, min delay 30 sec
Active is unknown
Forwarder 2
State is Init (standby RP, peer state is Active)
MAC address is 0007.b400.0102 (default)
Owner ID is aabb.cc00.0100
Preemption enabled, min delay 30 sec
Active is unknown
```

GLBP support for Stateful Switchover (SSO) mode is enabled by default but may be disabled by the **no glbp sso** command. If GLBP support for SSO mode is disabled, the output of the **show glbp** command on the standby RP will display a warning:

```
RouterRP-standby# show glbp

Ethernet0/0 - Group 1
State is Init (GLBP SSO disabled) <------ GLBP SSO is disabled.
```

```
Virtual IP address is 172.24.1.254
Hello time 3 sec, hold time 10 sec
Redirect time 600 sec, forwarder time-out 14400 sec
Preemption disabled
Active is unknown
Standby is unknown
Priority 100 (default)
Weighting 100 (default 100), thresholds: lower 1, upper 100
Load balancing: round-robin
Group members:
aabb.cc00.0100 (172.24.1.1) local
There are 2 forwarders (0 active)
Forwarder 1
State is Init (GLBP SSO disabled)
MAC address is 0007.b400.0101 (learnt)
Owner ID is aabb.cc00.0200
Preemption enabled, min delay 30 sec
Active is unknown
Forwarder 2
State is Init (GLBP SSO disabled)
MAC address is 0007.b400.0102 (default)
Owner ID is aabb.cc00.0100
Preemption enabled, min delay 30 sec
Active is unknown
```

Table 84 describes the significant fields shown in the displays.

Table 84 show glbp Field Descriptions

Field	Description
FastEthernet0/0 - Group	Interface type and number and GLBP group number for the interface.
State is	State of the virtual gateway or virtual forwarder. For a virtual gateway, the state can be one of the following: • Active—The gateway is the active virtual gateway (AVG) and is responsible for responding to Address Resolution Protocol (ARP) requests for the virtual IP address. • Disabled—The virtual IP address has not been configured or learned yet, but another GLBP configuration exists. • Initial—The virtual IP address has been configured or learned, but virtual gateway configuration is not complete. An interface must be up and configured to route IP, and an interface IP address must be configured. • Listen—The virtual gateway is receiving hello packets and is ready to change to the “speak” state if the active or standby virtual gateway becomes unavailable. • Speak—The virtual gateway is attempting to become the active or standby virtual gateway. • Standby—The gateway is next in line to be the AVG.

Table 84 show glbp Field Descriptions (continued)

Field	Description
	For a virtual forwarder, the state can be one of the following: • Active—The gateway is the active virtual forwarder (AVF) and is responsible for forwarding packets sent to the virtual forwarder MAC address. • Disabled—The virtual MAC address has not been assigned or learned. This is a transitory state because a virtual forwarder changing to a disabled state is deleted. • Initial—The virtual MAC address is known, but virtual forwarder configuration is not complete. An interface must be up and configured to route IP, an interface IP address must be configured, and the virtual IP address must be known. • Listen—The virtual forwarder is receiving hello packets and is ready to change to the "active" state if the AVF becomes unavailable.
Virtual IP address is	The virtual IP address of the GLBP group. All secondary virtual IP addresses are listed on separate lines. If one of the virtual IP addresses is a duplicate of an address configured for another device, it will be marked as "duplicate." A duplicate address indicates that the router has failed to defend its ARP cache entry.
Hello time, hold time	The hello time is the time between hello packets (in seconds or milliseconds). The hold time is the time (in seconds or milliseconds) before other routers declare the active router to be down. All routers in a GLBP group use the hello- and hold-time values of the current AVG. If the locally configured values are different, the configured values appear in parentheses after the hello- and hold-time values.
Next hello sent in	The time until GLBP will send the next hello packet (in seconds or milliseconds).
Preemption	Whether GLBP gateway preemption is enabled. If enabled, the minimum delay is the time (in seconds) for which a higher-priority nonactive router will wait before preempting the lower-priority active router. This field is also displayed under the forwarder section where it indicates GLBP forwarder preemption.
Active is	The active state of the virtual gateway. The value can be "local," "unknown," or an IP address. The address (and the expiration date of the address) is the address of the current AVG. This field is also displayed under the forwarder section where it indicates the address of the current AVF.
Standby is	The standby state of the virtual gateway. The value can be "local," "unknown," or an IP address. The address (and the expiration date of the address) is the address of the standby gateway (the gateway that is next in line to be the AVG).
Weighting	The initial weighting value with lower and upper threshold values.
Track object	The list of objects that are being tracked and their corresponding states.
IP redundancy name is	The name of the GLBP group.

Related Commands

Command	Description
glbp ip	Enables GLBP.
glbp timers	Configures the time between hello messages and the time before other routers declare the active GLBP router to be down.
glbp weighting track	Specifies an object to be tracked that affects the weighting of a GLBP gateway.

show interfaces accounting

To display the number of packets of each protocol type that have been sent through all configured interfaces, use the **show interfaces accounting** command in user EXEC or privileged EXEC mode.

show interfaces [*interface type number* | **null** *interface-number* | **vlan** *vlan-id*] **accounting**

Syntax Description

interface	(Optional) Interface type; possible valid values are **ethernet**, **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **pos**, and **port-channel**, **atm**, and **ge-wan**.
type number	(Optional) Module and port number; see the "Usage Guidelines" section for valid values.
null *interface-number*	(Optional) Specifies the null interface; the valid value is **0**.
vlan *vlan-id*	(Optional) Specifies the VLAN ID; valid values are from 1 to 4094.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(17a)SX1	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 12.2(33)SRA.
12.2(33)SRC	Support for IPv6 was added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

Note The Pkts Out and Chars Out fields display IPv6 packet counts only. The Pkts In and Chars In fields display both IPv4 and IPv6 packet counts, except for tunnel interfaces. For tunnel interfaces, the IPv6 input packets are counted as IPv6 packets only.

Due to hardware limitations on the ASIC, PFC IPv4 and IPv6 packets cannot be differentiated in the Pkts In and Chars In fields for IP count the IPv6 and IPv4 packets that are hardware forwarded. The Pkts In and Chars In fields for IPv6 only count software-forwarded packets. The IP Pkts Out and Chars Out fields show IPv4 packets, and the IPv6 Pkts Out and Chars Out fields show IPv6 packets.

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.

The port channels from 257 to 282 are internally allocated and are supported on the CSM and the FWSM only.

If you do not enter any keywords, all counters for all modules are displayed.

Examples

This example shows how to display the number of packets of each protocol type that have been sent through all configured interfaces:

```
Router> show interfaces gigabitethernet 5/2 accounting

GigabitEthernet5/2
Protocol  Pkts In  Chars In  Pkts Out  Chars Out
IP        50521    50521000  0         0
DEC MOP   0        0         1         129
CDP       0        0         1         592
IPv6      11       834       96        131658
Router#
```

Table 85 describes the significant fields shown in the display.

Table 85 show interfaces accounting Command Output Fields

Field	Description
Protocol	Protocol that is operating on the interface.
Pkts In	For IP it is the number of IPv4 software switched, IPv4 and IPv6 hardware switched packets received for the specified protocol. For IPv6 it is the number of IPv6 software switched packets received for the specified protocol.
Chars In	For IP it is the number of IPv4 software switched, IPv4 and IPv6 hardware switched characters received for the specified protocol. For IPv6 it is the number of IPv6 software switched characters received for the specified protocol.
Pkts Out	For IP it is the number of IPv4 sofware and hardware switched packets transmitted for the specified protocol. For IPv6 it is the number of IPv6 sofware and hardware switched packets transmitted for the specified protocol.
Chars Out	For IP it is the number of IPv4 software and hardware switched characters transmitted for the specified protocol. For IPv6 it is the number of IPv6 software and hardware switched characters transmitted for the specified protocol.

Related Commands

Command	Description
show interfaces	Displays the status and statistics for the interfaces in the chassis.

show ip sockets

To display IP socket information, use the **show ip sockets** command in user EXEC or privileged EXEC mode.

show ip sockets

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
10.0 T	This command was introduced.
12.2(2)T	Support for IPv6 socket information in the display output of the command was added.
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 Release 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.
12.4(11)T	This command was replaced by the **show udp**, **show sockets** and **show ip sctp** commands.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Use this command to verify that the socket being used is opening correctly. If there is a local and remote endpoint, a connection is established with the ports indicated.

Examples

The following is sample output from the **show ip sockets** command:

```
Router# show ip sockets

Proto    Remote          Port      Local           Port  In Out Stat TTY OutputIF
 17      10.0.0.0          0       172.16.186.193  67    0   0    1   0
 17      172.16.191.135   514      172.16.191.129  1811  0   0    0   0
 17      172.16.135.20    514      172.16.191.1    4125  0   0    0   0
 17      172.16.207.163   49       172.16.186.193  49    0   0    9   0
 17      10.0.0.0         123      172.16.186.193  123   0   0    1   0
 88      10.0.0.0         0        172.16.186.193  202   0   0    0   0
 17      172.16.96.59     32856    172.16.191.1    161   0   0    1   0
 17     --listen--              --any--         496  0    0   1    0
```

The following sample output from the **show ip sockets** command shows IPv6 socket information:

```
Router# show ip sockets

Proto      Remote     Port      Local      Port      In      Out      Stat      TTY OutputIF
17(v6)   --listen--           --any--    1024       0       0         0          0
17(v6)   --listen--           --any--       7       0       0         0          0
17(v6)   --listen--           --any--     161       0       0         0          0
17(v6)   --listen--           --any--     162       0       0         0          0
17       --listen--           --any--    1024       0       0         0          0
17       --listen--           --any--       7       0       0         0          0
17       --listen--           --any--       9       0       0         0          0
17       --listen--           --any--      19       0       0         0          0
17       --listen--           --any--    1645       0       0         0          0
17       --listen--           --any--    1646       0       0         0          0
17       --listen--           --any--     161       0       0         0          0
17       --listen--           --any--     162       0       0         0          0
```

Table 86 describes the significant fields shown in the display.

Table 86 show ip sockets Field Descriptions

Field	Description
Proto	Protocol type, for example, User Datagram Protocol (UDP) or TCP.
Remote	Remote address connected to this networking device. If the remote address is considered illegal, “--listen--” is displayed.
Port	Remote port. If the remote address is considered illegal, “--listen--” is displayed.
Local	Local address. If the local address is considered illegal or is the address 0.0.0.0, “--any--” displays.
Port	Local port.
In	Input queue size.
Out	Output queue size.
Stat	Various statistics for a socket.
TTY	The tty number for the creator of this socket.
OutputIF	Output IF string, if one exists.
v6	IPv6 sockets.

Related Commands

Command	Description
show ip sctp	Displays information about SCTP.
show processes	Displays information about the active processes.
show sockets	Displays IP socket information.
show udp	Displays IP socket information about UDP processes.

show ipv6 access-list

To display the contents of all current IPv6 access lists, use the **show ipv6 access-list** command in user EXEC or privileged EXEC mode.

show ipv6 access-list [*access-list-name*]

Syntax Description

access-list-name	(Optional) Name of access list.

Command Default

All IPv6 access lists are displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(2)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.
12.0(23)S	The priority field was changed to sequence and Layer 4 protocol information (extended IPv6 access list functionality) was added to the display output.
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.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
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.
12.2(50)SY	This command was modified. Information about IPv4 and IPv6 hardware statistics is displayed.

Usage Guidelines

The **show ipv6 access-list** command provides output similar to the **show ip access-list** command, except that it is IPv6-specific.

Examples

The following output from the **show ipv6 access-list** command shows IPv6 access lists named inbound, tcptraffic, and outbound:

```
Router# show ipv6 access-list

IPv6 access list inbound
    permit tcp any any eq bgp reflect tcptraffic (8 matches) sequence 10
    permit tcp any any eq telnet reflect tcptraffic (15 matches) sequence 20
    permit udp any any reflect udptraffic sequence 30
```

```
IPv6 access list tcptraffic (reflexive) (per-user)
    permit tcp host 2001:0DB8:1::1 eq bgp host 2001:0DB8:1::2 eq 11000 timeout 300 (time
        left 243) sequence 1
    permit tcp host 2001:0DB8:1::1 eq telnet host 2001:0DB8:1::2 eq 11001 timeout 300
        (time left 296) sequence 2

IPv6 access list outbound
    evaluate udptraffic
    evaluate tcptraffic
```

The following sample output shows IPv6 access list information for use with IPSec:

```
Router#  show ipv6 access-list
IPv6 access list Tunnel0-head-0-ACL (crypto)
     permit ipv6 any any (34 matches) sequence 1
IPv6 access list Ethernet2/0-ipsecv6-ACL (crypto)
     permit 89 FE80::/10 any (85 matches) sequence 1
```

Table 87 describes the significant fields shown in the display.

Table 87 show ipv6 access-list Field Descriptions

Field	Description
ipv6 access list inbound	Name of the IPv6 access list, for example, inbound.
permit	Permits any packet that matches the specified protocol type.
tcp	Transmission Control Protocol. The higher-level (Layer 4) protocol type that the packet must match.
any	Equal to ::/0.
eq	An equal operand that compares the source or destination ports of TCP or UDP packets.
bgp	Border Gateway Protocol. The lower-level (Layer 3) protocol type that the packet must be equal to.
reflect	Indicates a reflexive IPv6 access list.
tcptraffic (8 matches)	The name of the reflexive IPv6 access list and the number of matches for the access list. The **clear ipv6 access-list** privileged EXEC command resets the IPv6 access list match counters.
sequence 10	Sequence in which an incoming packet is compared to lines in an access list. Lines in an access list are ordered from first priority (lowest number, for example, 10) to last priority (highest number, for example, 80).
host 2001:0DB8:1::1	The source IPv6 host address that the source address of the packet must match.
host 2001:0DB8:1::2	The destination IPv6 host address that the destination address of the packet must match.
11000	The ephemeral source port number for the outgoing connection.
timeout 300	The total interval of idle time (in seconds) after which the temporary IPv6 reflexive access list named tcptraffic will time out for the indicated session.

Table 87 show ipv6 access-list Field Descriptions (continued)

Field	Description
(time left 243)	The amount of idle time (in seconds) remaining before the temporary IPv6 reflexive access list named tcptraffic is deleted for the indicated session. Additional received traffic that matches the indicated session resets this value to 300 seconds.
evaluate udptraffic	Indicates the IPv6 reflexive access list named udptraffic is nested in the IPv6 access list named outbound.

Related Commands

Command	Description
clear ipv6 access-list	Resets the IPv6 access list match counters.
hardware statistics	Enables the collection of hardware statistics.
show ip access-list	Displays the contents of all current IP access lists.
show ip prefix-list	Displays information about a prefix list or prefix list entries.
show ipv6 prefix-list	Displays information about an IPv6 prefix list or IPv6 prefix list entries.

show ipv6 cef

To display entries in the IPv6 Forwarding Information Base (FIB), use the **show ipv6 cef** command in user EXEC or privileged EXEC mode.

Privileged EXEC Mode

show ipv6 cef [*interface-type number* [**platform**] [**checksum** | **detail** | **internal** [**checksum**]] | *ipv6-prefix*[*/prefix-length*] [**dependents** | **longer-prefixes** [**platform**] [**checksum** | **detail** | **internal** [**checksum**]] | **similar-prefixes** | **platform** [**checksum** | **detail** | **internal** [**checksum**]] | **epoch** | **prefix-statistics** | **checksum** | **detail** | **internal** [**checksum**]]

User EXEC Mode

show ipv6 cef [*ipvg-prefix*[*/prefix-length*] [**dependents** | **detail** | **longer-prefixes** [**platform**] [**detail**] | **similar-prefixes**] | *interface-type interface-number* [**platform**] [**detail**] | **epoch** | **prefix-statistics**]

Syntax Description

ipv6-prefix	(Optional) IPv6 network assigned to the interface. • This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/prefix-length	(Optional) The IPv6 network assigned to the interface and the length of the IPv6 prefix. • The *ipv6-prefix* must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons. The *prefix-length* is a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
longer-prefixes	(Optional) Displays FIB information for more specific destinations.
interface-type	(Optional) Interface type. For more information, use the question mark (?) online help function.
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.
platform	(Optional) Displays platform-specific Cisco Express Forwarding data.
detail	(Optional) Displays detailed FIB entry information.
internal	(Optional) Displays internal FIB entry information.
checksum	(Optional) Displays FIB entry checksums.
dependents	(Optional) Displays dependents of the selected prefix.
similar-prefixes	(Optional) Displays FIB information for prefixes that are similar to one another.
epoch	(Optional) Displays the basic FIB entries filtered by epoch number.
summary	(Optional) Displays the summary of events log.

new	(Optional) Displays new events since the last show operation was performed.
within *minutes*	(Optional) Displays events within the specified time, in minutes. The range is from 1 to 4294967295.
prefix-statistics	(Optional) Displays nonzero prefix statistics.

Command Default

If no keyword or argument is specified, information about all FIB entries is displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(21)ST	This command was introduced.
12.0(22)S	This command was modified. The *interface-type* and *interface-number* arguments and the **longer-prefixes** and **detail** keywords were added.
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(25)S	This command was modified. The **dependents**, **events**, **internal, new, platform**, **similar-prefixes** and **within** 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.
12.2(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

The **show ipv6 cef** command is similar to the **show ip cef** command, except that it is IPv6-specific.

Examples

The following is sample output from the **show ipv6 cef** command when no keywords or arguments are entered:

```
Router# show ipv6 cef

Global IPv6 CEF Table
12 prefixes

2FFE::3/128
  Receive
2FFE::/64
  attached to POS3/1
3FFE::/64
  nexthop FE80::yyyy:4AFF:FE6D:B980 POS3/1
  nexthop FE80::xxxx:7DFF:FE8D:A840 FastEthernet1/0
3FFE:zz::3/128
  Receive
3FFE:zz::/64
```

```
  attached to FastEthernet1/0
3FFE:rr::3/128
  Receive
3FFE:rr::/64
  attached to FastEthernet1/1
3FFE:pp::3/128
  Receive
3FFE:pp::/64
  attached to FastEthernet1/2
3FFE:nnnn:2222::/64
  nexthop::POS3/1
3FFE:ssss::/64
  recursive via 2FFE::2 POS3/1
FE80::/64
  Receive
```

The following is sample output from the **show ipv6 cef** command showing 6PE multipath information:

```
Router# show ipv6 cef

Global IPv6 CEF Table
12 prefixes
.
.
.
nexthop 10.1.1.3 Ethernet0/0 label 25 16
4004::/64
  nexthop 10.1.1.3 Ethernet0/0 label 27 16
  nexthop 10.1.1.3 Ethernet0/0 label 26 18
```

Table 88 describes the significant fields shown in the displays.

Table 88 show ipv6 cef Field Descriptions

Field	Description
12 prefixes	Indicates the total number of IPv6 prefixes in the Cisco Express Forwarding table.
2FFE::3/128	Indicates the IPv6 prefix of the remote network.
Receive	Indicates that this IPv6 prefix is local to the router.
3FFE::/64 nexthop FE80::yyyy:4AFF:FE6D:B980 POS3/1 nexthop FE80::xxxx:7DFF:FE8D:A840 FastEthernet1/0	Indicates that IPv6 prefix 3FFE::/64 is reachable through these next hop addresses and interfaces. • Multiple next-hop entries are shown for IPv6 prefixes that have load sharing.
attached to FastEthernet1/0	Indicates that this IPv6 prefix is a connected network on Fast Ethernet interface 1/0.
recursive via 2FFE::2 POS3/1	Indicates that this IPv6 prefix uses the same forwarding information as 2FFE::2 POS3/1.

The following is sample output from the **show ipv6 cef detail** command for Fast Ethernet interface 1/0:

```
Router# show ipv6 cef fastethernet 1/0 detail

IPv6 CEF is enabled and running
IPv6 CEF default table
2 prefixes
3FFE:zz::/64
```

```
  attached to FastEthernet1/0
3FFE:rr::/64
  attached to FastEthernet1/1
```

The fields in the are self-explanatory.

The following is sample output from the **show ipv6 cef longer-prefixes** command for the IPv6 prefix 3FFE:xxxx:20:1::12/128. The fields in the display are self-explanatory.

```
Router# show ipv6 cef 3FFE:xxxx:20:1::12/128 longer-prefixes

IPv6 CEF is enabled and running
IPv6 CEF default table
2 prefixes
3FFE:xxxx:20:1::12/128 Receive
  Receive
3FFE:xxxx:20:1::/64 Attached, Connected
     attached to Tunnel81
```

The following is sample output from the **show ipv6 cef detail** command showing 6PE multipath information. The prefix 4004::/64 is received by the Border Gateway Protocol (BGP) from two different peers and therefore two different paths.

```
Router# show ipv6 cef detail

IPv6 CEF is enabled and running
VRF Default:
 20 prefixes (20/0 fwd/non-fwd)
 Table id 0, version 20, 0 resets
 Database epoch:0 (20 entries at this epoch)
.
.
.
4004::/64, epoch 0, per-destination sharing
  recursive via 172.11.11.1 label 27
    nexthop 10.1.1.3 Ethernet0/0 label 16
  recursive via 172.30.30.1 label 26
    nexthop 10.1.1.3 Ethernet0/0 label 18
```

The fields in the display are self-explanatory.

The following is sample output from the **show ipv6 cef internal** command:

```
Router# show ipv6 cef internal

IPv6 CEF is enabled and running
Slow processing intvl = 1 seconds backoff level current/max 0/0
0 unresolved prefixes, 0 requiring adjacency update
IPv6 CEF default table
14 prefixes tableid 0
table version 17
root 6283F5D0
.
.
.
BEEF:20::/64 RIBfib  <======================entry with two mpls path
 Using loadinfo 0x62A75194
  loadinfo ptr 62A75194 flags 0000 next hash  = 0
  refcount 3 path list ptr 0x00000000
  hashes :-
      62335678  drop adjacency
     .
     .
     .
  path list pointer 62370FA0
```

```
    2 paths -
     Nexthop  path_pointer 6236E420 traffic share 1 path_list pointer 62370FA0
     nexthop ::FFFF:172.12.12.1
     next_hop_len 0 adjacency pointer 62335678
     Nexthop  path_pointer 6236E480 traffic share 1 path_list pointer 62370FA0
     nexthop ::FFFF:172.14.14.1
     next_hop_len 0 adjacency pointer 62335678
    refcount 2
    1 loadinfos -
     loadinfo ptr 62A75194 flags 0000 next hash  = 0
     refcount 3 path list ptr 0x00000000
     hashes :-
       62335678  drop adjacency
      .
      .
      .
  tag information
    local tag: exp-null
    rewrites :-
       Fa0/1, 10.2.1.1, tags imposed: {32}
       Fa1/0, 10.1.1.3, tags imposed: {25}
       Fa0/1, 10.2.1.1, tags imposed: {32}
       Fa1/0, 10.1.1.3, tags imposed: {25}
       Fa0/1, 10.2.1.1, tags imposed: {32}
       Fa1/0, 10.1.1.3, tags imposed: {25}
       Fa0/1, 10.2.1.1, tags imposed: {32}
       Fa1/0, 10.1.1.3, tags imposed: {25}
       Fa0/1, 10.2.1.1, tags imposed: {32}
       Fa1/0, 10.1.1.3, tags imposed: {25}
       Fa0/1, 10.2.1.1, tags imposed: {32}
       Fa1/0, 10.1.1.3, tags imposed: {25}
FE80::/10 Receive, RIBfib
  Receive
FF00::/8 Receive, RIBfib
  Receive
```

Table 88 and Table 89 describe the significant fields shown in displays.

Table 89 show ipv6 cef internal Field Descriptions

Field	Description
Slow processing intvl	Displays the slow processing interval, in seconds.
backoff level current/max	Displays the backoff level in the ratio current to the maximum backoff value.
unresolved prefixes	Displays the total number of unresolved prefixes.
requiring adjacency update	Indicates the number of prefixes that have been resolved but the associated forwarding information has not yet been updated to reflect the route resolution.
prefixes	Total number of prefixes in the IPv6 Cisco Express Forwarding default table.
tableid	ID of the IPv6 Cisco Express Forwarding default table.
table version	Version of the IPv6 Cisco Express Forwarding default table.

Table 89 show ipv6 cef internal Field Descriptions (continued)

Field	Description
root	Root number of the IPv6 Cisco Express Forwarding default table.
Using loadinfo	Current load information
loadinfo ptr	Load information pointer.
flags	Total number of flags.
next hash	Next hash value.
refcount 3 path list ptr	Location of the refcount 3 path list pointer.
hashes	Total number of hashes.
Nexthop path_pointer	Location of the next hop path pointer.
path_list pointer	Location of the path list pointer.
refcount	Location of the reference counter.
loadinfo ptr	Location of the load information pointer.

The following is sample output from the **show ipv6 cef internal** command showing 6PE multipath information. The fields in the display are self-explanatory.

```
Router# show ipv6 cef internal

4004::/64, version 15, epoch 0, RIB, refcount 3, per-destination sharing
  sources:RIB
  feature space:
   IPRM:0x00028000
  path 01A53DA0, path list 01A4F2E0, share 0, flags recursive, resolved
  ifnums:(none)
   path_list contains no resolved destination(s). HW IPv4 notified.
  recursive via 172.11.11.1 label 27, fib 01A6CCA0, 1 terminal fib
    path 01A540B0, path list 01A4F5F0, share 1, flags nexthop
    ifnums:(none)
     path_list contains no resolved destination(s). HW IPv4 notified.
    nexthop 10.1.1.3 Ethernet0/0 label 16, mask /0, adjacency IP adj out of
Ethernet0/0, addr 10.1.1.3 01DE9FB0
  path 01A53D30, path list 01A4F2E0, share 0, flags recursive, resolved
  ifnums:(none)
   path_list contains no resolved destination(s). HW IPv4 notified.
  recursive via 172.30.30.1 label 26, fib 01A6CBD0, 1 terminal fib
    path 01A540B0, path list 01A4F5F0, share 1, flags nexthop
    ifnums:(none)
     path_list contains no resolved destination(s). HW IPv4 notified.
    nexthop 10.1.1.3 Ethernet0/0 label 18, mask /0, adjacency IP adj out of
Ethernet0/0, addr 10.1.1.4 01DE9FB0
  output chain:
    loadinfo 01A47520, per-session, flags 0011, 2 locks
    flags:Per-session, for-mpls-not-at-eos
    16 hash buckets
      <0  > label 27 label 16 TAG adj out of Ethernet0/0, addr 10.1.1.3
01DE9E30
      <1  > label 26 label 18 TAG adj out of Ethernet0/0, addr 10.1.1.3
01DE9E30
      <2  > label 27 label 16 TAG adj out of Ethernet0/0, addr 10.1.1.3
01DE9E30
      <3  > label 26 label 18 TAG adj out of Ethernet0/0, addr 10.1.1.3
01DE9E30
```

```
      <4  > label 27 label 16 TAG adj out of Ethernet0/0, addr 10.1.1.3
.
.
.
      <15 > label 26 label 18 TAG adj out of Ethernet0/0, addr 10.1.1.3
01DE9E30
```

The following is sample output from the **show ipv6 cef** command, showing information about the Multiprotocol Label Switching (MPLS) labels associated with the FIB table entries for an IPv6 prefix that is configured to be a Cisco 6PE router using MPLS to transport IPv6 traffic over an IPv4 network.

To display label information from the Cisco Express Forwarding table, enter the **show ipv6 cef** command with an IPv6 prefix. The fields in the display are self-explanatory.

```
Router# show ipv6 cef 2001:0DB8::/32

2001:0DB8::/32
      nexthop ::FFFF:192.168.99.70
      fast tag rewrite with Se0/0, point2point, tags imposed {19 20}
fast tag rewrite with Se0/0, point2point, tags imposed {19 20}
```

Sample Output for Cisco IOS Releases 12.2(25)S, 12.2(28)SB, 12.2(33)SRA,12.2(33)SXH, 12.4(20)T, and Later Releases

The sample output in the following commands was reformatted with the implementation of Cisco Express Forwarding enhancements. The information in the output is the same as it was before the enhancements.

The following is sample output from the **show ipv6 cef internal** command:

```
Router# show ipv6 cef internal

IPv6 CEF is enabled and running
VRF Default:
 20 prefixes (20/0 fwd/non-fwd)
 Table id 0, 0 resets
 Database epoch: 0 (20 entries at this epoch)

2001:1:12::/64, epoch 0, RIB, refcount 3
  sources: RIB
  feature space:
   MFI: path extension list empty
   IPRM: 0x00038000
   IPV6 adj out of POS1/0 635BAFE0
  path 633A9A18, path list 633A732C, share 1, type attached nexthop
  ifnums: (none)
   path_list contains at least one resolved destination(s). HW IPv6 notified.
  nexthop FE80::205:DCFF:FE26:4800 POS1/0, adjacency IPV6 adj out of POS1/0 635BAFE0
  output chain: IPV6 adj out of POS1/0 635BAFE0
```

The fields in the display are self-explanatory.

The following is sample output from the **show ipv6 cef** *ipv6-prefix*/*prefix-length* **internal** command:

```
Router# show ipv6 cef 2001:2:25::/64 internal

2001:2:25::/64 RIBfib
 Using cached adjacency 0x629E1CE0
  path list pointer 62A2C310
    1 path -
     Nexthop  path_pointer 62A297B0 traffic share 1 path_list pointer 62A2C310
     nexthop FE80::2D0:1FF:FEE4:6800 FastEthernet0/1
     next_hop_len 0 adjacency pointer 629E1CE0
    refcount 10
    no loadinfo
```

The following is sample output from the **show ipv6 cef detail** command. The fields in the display are self-explanatory.

```
Router# show ipv6 cef detail

IPv6 CEF is enabled and running
VRF Default:
 20 prefixes (20/0 fwd/non-fwd)
 Table id 0, 0 resets
 Database epoch: 0 (20 entries at this epoch)

2001:1:12::/64, epoch 0
  nexthop FE80::205:DCFF:FE26:4800 POS1/0
2001:2:13::/64, epoch 0, flags attached, connected
  attached to POS1/0
2001:2:13::2/128, epoch 0, flags receive
```

The following is sample output from the **show ipv6 cef epoch** command. The fields in the display are self-explanatory.

```
Router# show ipv6 cef epoch

Table: Default
 Database epoch: 1 (2 entries at this epoch)
```

Related Commands

Command	Description
show cef interface	Displays Cisco Express Forwarding-related interface information.
show ipv6 cef adjacency	Displays Cisco Express Forwarding for IPv6 recursive and direct prefixes resolved through an adjacency.
show ipv6 route	Displays IPv6 router advertisement information received from onlink routers.

show ipv6 cef adjacency

To display Cisco Express Forwarding for IPv6 and distributed Cisco Express Forwarding v6 recursive and direct prefixes resolved through an adjacency, use the **show ipv6 cef adjacency** command in user EXEC or privileged EXEC mode.

show ipv6 cef adjacency *interface-type interface-number ipv6-address* [**detail** | **internal** | **samecable**] [**platform** [**detail** | **internal** | **samecable**]] [**source** [**internal** | **epoch** *epoch-number* [**internal** | **samecable** | **platform** [**detail** | **internal** | **samecable**]]]] [**epoch** *epoch-number* [**internal** | **samecable** | **platform** [**detail** | **internal** | **samecable**]]]

To display Cisco Express Forwarding for IPv6 and distributed Cisco Express Forwarding v6 recursive and direct prefixes resolved through special adjacency types representing nonstandard switching paths, use this form of the **show ip cef adjacency** command in user EXEC or privileged EXEC mode.

show ipv6 cef adjacency {**adj-null** | **discard** | **drop** | **glean** | **null** | **punt**} [**checksum**] [**detail**] [**internal**] [**samecable**] [**platform** [**checksum** | **detail** | **internal** | **samecable**]] [**source** [**internal** | **epoch** *epoch-number* [**internal** | **samecable** | **platform** [**detail** | **internal** [**checksum**] | **samecable**]]]] [**epoch** *epoch-number* [**internal** | **samecable** | **detail** | **platform** [**detail** | **internal** | **samecable**]]]

Syntax Description

interface-type	Interface type for which to display Cisco Express Forwarding adjacency information.
interface-number	Interface number for which to display adjacency information.
ipv6-address	Next-hop IPv6 address. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
detail	(Optional) Displays detailed information for each CEFv6 adjacency type entry.
internal	(Optional) Displays data for adjacency type entries.
samecable	(Optional) Displays the connected (up) interface for adjacency type entries.
platform	(Optional) Displays platform-specific adjacency information.
source	(Optional) Displays source-specific adjacency information.
epoch *epoch-number*	(Optional) Displays adjacency type entries filtered by epoch number. The epoch number range is from 0 to 255.
discard	Displays discard adjacency information. Sets up for loopback interfaces. Loopback IPv6 addresses are receive entries in the FIB table.
drop	Displays drop adjacency information. Packets forwarded to this adjacency are dropped.
glean	Displays glean adjacency information. Represents destinations on a connected interface for which no Address Resolution Protocol (ARP) cache entry exists.
null	Displays null adjacency information. Formed for the null 0 interface. Packets forwarded to this adjacency are dropped.
punt	Displays punt adjacency information. Represents destinations that cannot be switched in the normal path and that are punted to the next fastest switching vector.

adj-null	Displays null adjacency information.
checksum	(Optional) Displays FIB entry checksums.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(22)S	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(25)S	This command was modified. The **internal**, **samecable**, **platform**, and **source** keywords were added.
12.2(28)SB	This command was modified. The **null** keyword was added.
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 ipv6 cef adjacency** command is similar to the **show ip cef adjacency** command, except that it is IPv6 specific.

This command shows all prefixes resolved through a regular next-hop adjacency or through a special adjacency type such as discard, drop, glean, null, and punt. An adjacency is a node that can be reached by one Layer 2 hop.

Examples

The following is sample output from the **show ipv6 cef adjacency** command when the **glean** type is specified:

```
Router# show ipv6 cef adjacency glean

Prefix              Next Hop             Interface
3FFE:xxxx::/24       attached             Ethernet1
2002::/16           3FFE:xxxx::1          Ethernet1
```

The following is sample output from the **show ipv6 cef adjacency drop** command with **detail** specified:

```
Router# show ipv6 cef adjacency fastethernet 0/1 drop detail

IPv6 CEF is enabled and running
IPv6 CEF default table
12 prefixes
```

The following sample output shows the direct IPv6 prefix when next-hop Ethernet interface 1 is specified:

```
Router# show ipv6 cef adjacency ethernet 1 3FFE:xxxx::250:8BFF:FEE8:F800

Prefix                                    Next Hop             Interface
3FFE:xxxx::250:8BFF:FEE8:F800/128         2002::/16          Ethernet1
```

Table 90 describes the fields shown in the display.

Table 90 show ipv6 cef adjacency Field Descriptions

Field	Description
Prefix	Destination IPv6 prefix.
Next Hop	Next-hop IPv6 address.
Interface	Next-hop interface.

Related Commands

Command	Description
show ipv6 cef summary	Displays a summary of the entries in the IPv6 FIB.

show ipv6 cef neighbor discovery throttling

To display the Cisco Express Forwarding for IPv6 neighbor discovery (ND) throttling list, use the **show ipv6 cef neighbor discovery throttling** command in privileged EXEC mode.

show ipv6 cef neighbor discovery throttling [**internal**]

Syntax Description

internal	(Optional) Displays internal data structures.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following is sample output from the **show ipv6 cef neighbor discovery throttling** command:

```
Router# show ipv6 cef neighbor discovery throttling

Address                                   Holdtime
2001:1111::1                              00:00:02.296
```

Table 91 describes the fields shown in the display.

Table 91 show ipv6 cef neighbor discovery throttling Field Descriptions

Field	Description
Address	The IPv6 address for which the information on ND throttling list is displayed.
Holdtime	Length of time (in hours, minutes, and seconds) that the Cisco IOS software will wait to hear from the peer before declaring it down.

Related Commands

Command	Description
show ipv6 neighbors	Displays IPv6 ND cache information.

show ipv6 cef non-recursive

To display nonrecursive route entries in the IPv6 Forwarding Information Base (FIB), use the **show ipv6 cef non-recursive** command in user EXEC or privileged EXEC mode.

show ipv6 cef non-recursive [**detail** | **internal** | **samecable**] [**platform** [**detail** | **internal** | **samecable**]] [**source** [**internal** | **epoch** *epoch-number* [**internal** | **samecable** | **platform** [**detail** | **internal** | **samecable**]]]] [**epoch** *epoch-number* [**internal** | **samecable** | **platform** [**detail** | **internal** | **samecable**]]]

Syntax Description

detail	(Optional) Displays detailed nonrecursive route entry information.
internal	(Optional) Displays data for nonrecursive route entries.
samecable	(Optional) Displays the connected (up) interface for nonrecursive route entries.
platform	(Optional) Displays platform-specific nonrecursive route entries.
source	(Optional) Displays source-specific nonrecursive route entry information.
epoch *epoch-number*	(Optional) Displays adjacency type entries filtered by epoch number. The epoch number range is from 0 to 255.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(22)S	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(25)S	The **internal**, **samecable**, **platform**, **source**, and **epoch** keywords were added, and the *epoch-number* argument was added. Next hop information was removed from the command output.
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(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The **show ipv6 cef non-recursive** command is similar to the **show ip cef non-recursive** command, except that it is IPv6-specific.

The **show ipv6 cef non-recursive detail** command shows detailed FIB entry information for all nonrecursive routes.

Examples

The following is sample output from the **show ipv6 cef non-recursive detail** command:

```
Router# show ipv6 cef non-recursive detail

IPv6 CEF is enabled and running
IPv6 CEF default table
8 prefixes
2001:xx::/35
     nexthop FE80::ssss:CFF:FE3D:DCC9 Tunnel55
2001:zzz:500::/40
     nexthop FE80::nnnn:801A Tunnel32
2001:zzz::/35
     nexthop 3FFE:mmm:8023:21::2 Tunnel26
3FFE:yyy:8023:37::1/128 Receive
  Receive
3FFE:yyy:8023:37::/64 Attached, Connected
     attached to Tunnel37
3FFE:yyy:8023:38::1/128 Receive
  Receive
3FFE:yyy:8023:38::/64 Attached, Connected
     attached to Tunnel40
3FFE:yyy:8023:39::1/128 Receive
  Receive
```

Table 92 describes the significant fields shown in the display.

Table 92 show ipv6 cef non-recursive Field Descriptions

Field	Description
8 prefixes	Indicates the total number of IPv6 prefixes in the Cisco Express Forwarding table.
2001:xx::/35	Indicates the IPv6 prefix of the remote network.
2001:zzz:500::/40 nexthop FE80::nnnn:801A Tunnel32	Indicates that IPv6 prefix 2001:zzz:500::/40 is reachable through this next-hop address and interface.
attached to Tunnel37	Indicates that this IPv6 prefix is a connected network on Tunnel interface 37.
Receive	Indicates that this IPv6 prefix is local to the router.

This is an example of the **show ipv6 cef non-recursive** command output in Cisco IOS Releases 12.2(25)S, 12.2(28)SB, 12.2(33)SRA, 12.2(33)SXH, 12.4(20)T, and later releases:

```
Router# show ipv6 cef non-recursive

2003:1::/64
  attached to POS6/1/0
2003:1::1/128
  receive
2003:2::/64
  attached to Loopback0
2003:2::1/128
```

Related Commands

Command	Description
show ipv6 cef	Displays entries in the IPv6 FIB.
show ipv6 cef summary	Displays a summary of the entries in the IPv6 forwarding FIB.
show ipv6 cef unresolved	Displays unresolved entries in the IPv6 FIB.

show ipv6 cef platform

To display platform-specific Cisco Express Forwarding data, use the **show ipv6 cef platform** command in user EXEC or privileged EXEC mode.

show ipv6 cef platform [**detail** | **internal** | **samecable**]

Syntax Description

detail	(Optional) Displays detailed platform-specific Cisco Express Forwarding data.
internal	(Optional) Displays internal platform-specific Cisco Express Forwarding data.
samecable	(Optional) Displays platform-specific data for the connected (up) interface.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(22)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SCE	This command was integrated into Cisco IOS Release 12.2(33)SCE.

Usage Guidelines

If none of the optional keywords is used, data for all platforms is displayed.

Examples

The following example will display all platform-specific Cisco Express Forwarding data:

```
Router# show ipv6 cef platform
```

show ipv6 cef summary

To display a summary of the entries in the IPv6 Forwarding Information Base (FIB), use the **show ipv6 cef summary** command in user EXEC or privileged EXEC mode.

show ipv6 cef summary

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(22)S	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(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.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The **show ipv6 cef summary** command is similar to the **show ip cef summary** command, except that it is IPv6-specific.

Examples

The following is sample output from the **show ipv6 cef summary** command:

```
Router# show ipv6 cef summary

IPv6 CEF is enabled and running
Slow processing intvl = 1 seconds backoff level current/max 0/0
0 unresolved prefixes, 0 requiring adjacency update
IPv6 CEF default table
9 prefixes
```

Table 93 describes the significant fields shown in the display.

Table 93 show ipv6 cef summary Field Descriptions

Field	Description
Slow processing intvl	Indicates the waiting time (in seconds) before the software attempts to resolve any unresolved routes.

Table 93 show ipv6 cef summary Field Descriptions (continued)

Field	Description
unresolved prefixes	Indicates the number of unresolved routes.
requiring adjacency update	Indicates the number of prefixes that have been resolved but the associated forwarding information has not yet been updated to reflect the route resolution.

This is an example of the **show ipv6 cef summary** command output in Cisco IOS Releases 12.2(25)S, 12.2(28)SB, 12.2(33)SRA, 12.2(33)SXH, 12.4(20)T, and later releases:

```
Router# show ipv6 cef summary

IPv6 CEF is enabled and running
VRF Default:
 20 prefixes (20/0 fwd/non-fwd)
 Table id 0, 0 resets
 Database epoch: 0 (20 entries at this epoch)
```

Related Commands

Command	Description
show ipv6 cef	Displays entries in the IPv6 FIB.
show cef interface	Displays Cisco Express Forwarding-related interface information.

show ipv6 cef switching statistics

To display switching statistics in the IPv6 Forwarding Information Base (FIB), use the **show ipv6 cef switching statistics** command in privileged EXEC mode.

show ipv6 cef switching statistics [**feature**]

Syntax Description

feature	(Optional) The output is ordered by feature.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(25)S	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.
12.2(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

If the optional feature keyword is not used, all switching statistics are displayed.

Examples

The following is sample output from the **show ipv6 cef switching statistics** command:

```
Router# show ipv6 cef switching statistics

Reason                                 Drop       Punt  Punt2Host
RP LES Packet destined for us             0     132248          0
RP LES Multicast                          0          2          0
RP LES Link-local                         0         33          0
RP LES Total                              0     132283          0

Slot 4 Packet destined for us             0     129546          0
Slot 4 Link-local                         0         31          0
Slot 4 Total                              0     129577          0

All    Total                              0     261860          0
```

Table 94 describes the significant fields shown in the display.

Table 94 show ipv6 cef switching statistics Field Descriptions

Field	Description
Reason	Packet description.
Drop	Number of packets dropped.

Table 94 show ipv6 cef switching statistics Field Descriptions (continued)

Field	Description
Punt	Number of packets that could be switched in the normal path and were punted to the next fastest switching vector.
Punt2Host	Number of packets that cannot be switched in the normal path and were punted to the host.

Related Commands

Command	Description
show cef interface	Displays Cisco Express Forwarding-related interface information.
show ipv6 cef	Displays entries in the IPv6 FIB.
show ipv6 route	Displays IPv6 router advertisement information received from onlink routers.

show ipv6 cef traffic prefix-length

To display Cisco Express Forwarding for IPv6 (CEFv6) and distributed CEFv6 (dCEFv6) traffic statistics, use the **show ipv6 cef traffic prefix-length** command in user EXEC or privileged EXEC mode.

show ipv6 cef traffic prefix-length

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(22)S	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(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.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The **show ipv6 cef traffic prefix-length** command is similar to the **show ip cef traffic prefix-length** command, except that it is IPv6-specific.

This command is used to display CEFv6 switched traffic statistics by destination prefix length. The **ipv6 cef accounting prefix-length** command must be enabled for the counters to increment.

Examples

The following is sample output from the **show ipv6 cef traffic prefix-length** command:

```
Router# show ipv6 cef traffic prefix-length

IPv6 prefix length switching statistics:
----------------------------------------
Prefix       Number of       Number of
Length       Packets         Bytes
----------------------------------------
     0               0               0
     1              24            3840
     2               0               0
     3              14            1120
     4               0               0
     5              10            1200
.
.
.
    28               0               0
```

```
29                4                512
30                0                0
31                18               2448
32                0                0
```

Table 95 describes the significant fields shown in the display.

Table 95 show ipv6 cef traffic prefix-length Field Descriptions

Field	Description
Prefix Length	Destination IPv6 prefix length for Cisco Express Forwarding switched traffic.
Number of Packets	Number of packets forwarded for the specified IPv6 prefix length.
Number of Bytes	Number of bytes sent for the specified IPv6 prefix length.

Related Commands

Command	Description
ipv6 cef accounting	Enables CEFv6 network accounting.
show ipv6 cef	Displays entries in the IPv6 FIB.
show ipv6 cef summary	Displays a summary of the entries in the IPv6 FIB.

show ipv6 cef tree

To display summary information on the default tree in the IPv6 Forwarding Information Base (FIB), use the **show ipv6 cef tree** command in user EXEC or privileged EXEC mode.

show ipv6 cef tree [**statistics** | **dependents** [*prefix-filter*]]

Syntax Description

statistics	(Optional) Displays the default tree statistics.
dependents	(Optional) Displays the dependents of the selected tree with optional prefix filter.
prefix-filter	(Optional) A prefix filter on the dependents of the selected tree.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(25)S	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.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

If none of the optional keywords or arguments is used, all summary information on the default tree in the IPv6 FIB is shown.

Examples

The following is sample output from the **show ipv6 cef tree** command:

```
Router# show ipv6 cef tree

VRF Default tree information:
 RTRIE storing IPv6 addresses
 6 entries (6/0 fwd/non-fwd)
 Forwarding & Non-forwarding tree:
  6 inserts, 0 delete
  8 nodes using 288 bytes
```

Table 96 describes the significant fields shown in the display.

Table 96 show ipv6 cef tree Field Descriptions

Field	Description
RTRIE storing IPv6 addresses	Indicates the tree type as RTRIE.
6 entries (6/0 fwd/non-fwd)	Indicates total number of prefix entries as 6 forwarding and 0 nonforwarding entries.

Table 96 show ipv6 cef tree Field Descriptions (continued)

Field	Description
Forwarding & Non-forwarding tree	Same tree is used for forwarding and nonforwarding.
6 inserts, 0 delete	Indicates that 6 entries were inserted and 0 entries were deleted from the tree.
8 nodes using 288 bytes	Indicates a total of 8 nodes using a total of 288 bytes of memory.
*calloc failures: *number* node	This line is not present in the example output. If this line is present in output, it indicates a memory allocation error at the indicated node.

Related Commands

Command	Description
show ipv6 cef	Displays entries in the IPv6 FIB.

show ipv6 cef unresolved

To display unresolved entries in the IPv6 Forwarding Information Base (FIB), use the **show ipv6 cef unresolved** command in user EXEC or privileged EXEC mode.

show ipv6 cef unresolved [**detail** | **internal** | **samecable**] [**platform** [**detail** | **internal** | **samecable**]] [**source** [**internal** | **epoch** *epoch-number* [**internal** | **samecable** | **platform** [**detail** | **internal** | **samecable**]]]] [**epoch** *epoch-number* [**internal** | **samecable** | **platform** [**detail** | **internal** | **samecable**]]]

Syntax Description

detail	(Optional) Displays detailed FIB entry information.
internal	(Optional) Displays data structures for unresolved routes.
samecable	(Optional) Displays the connected (up) interface for unresolved routes.
platform	(Optional) Displays platform-specific information on unresolved routes.
source	(Optional) Displays source-specific information on unresolved routes.
epoch *epoch-number*	(Optional) Displays the basic unresolved routes filtered by a specified epoch number. The epoch number range is from 0 to 255.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(22)S	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(25)S	The **internal**, **samecable**, **platform**, **source**, and **epoch** keywords were added. The *epoch-number* argument 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.
12.2(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

The **show ipv6 cef unresolved** command is similar to the **show ip cef unresolved** command, except that it is IPv6-specific.

The **show ipv6 cef unresolved detail** command displays detailed information for all unresolved FIB entries.

Examples

The following is sample output from the **show ipv6 cef unresolved** command with the **detail** keyword:

```
Router# show ipv6 cef unresolved detail

IPv6 CEF is enabled for distributed  and running
VRF Default:
 5 prefixes (5/0 fwd/non-fwd)
 Table id 0, version 5, 0 resets
 Database epoch: 2 (5 entries at this epoch)
```

Table 79 describes the significant fields shown in the display.

Table 97 show ipv6 cef unresolved Field Descriptions

Field	Description
5 prefixes (5/0 fwd/non-fwd)	Indicates how many IPv6 prefixes are being used for forwarding or not forwarding.
Table id 0, version 5, 0 resets	Provides information about the Cisco Express Forwarding table.
Database epoch: 2 (5 entries at this epoch)	The epoch number of any unresolved database epochs.

This is an example of the **show ipv6 cef unresolved detail** command output in Cisco IOS Releases 12.2(25)S, 12.2(28)SB, 12.2(33)SRA, 12.2(33)SXH, 12.4(20)T, and later releases:

```
Router# show ipv6 cef unresolved detail
```

No unresolved adjacencies exist, therefore nothing is displayed in the output of the **show ipv6 cef unresolved detail** command.

Related Commands

Command	Description
show cef interface	Displays Cisco Express Forwarding-related interface information.
show ipv6 cef	Displays entries in the IPv6 FIB.
show ipv6 cef summary	Displays a summary of the entries in the IPv6 FIB.

show ipv6 cef vrf

To display the Cisco Express Forwarding Forwarding Information Base (FIB) associated with an IPv6 Virtual Private Network (VPN) routing and forwarding (VRF) instance, use the **show ipv6 cef vrf** command in user EXEC or privileged EXEC mode.

show ipv6 cef vrf [*vrf-name* | ***** | **internal**]

Syntax Description

vrf-name	(Optional) Name assigned to the VRF.
*	(Optional) All VRFs are displayed.
internal	(Optional) Only internal data is displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.2(33)SRB1	This command was integrated into Cisco IOS Release 12.2(33)SRB1.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Use the **show ipv6 cef vrf** command to display content of the IPv6 FIB for the specified VRF.

Examples

The following is sample output from a Cisco Express Forwarding FIB associated with a VRF named cisco1:

```
Router# show ipv6 cef vrf cisco1

 2001:8::/64
  attached to FastEthernet0/0
 2001:8::3/128
  receive
 2002:8::/64
  nexthop 10.1.1.2 POS4/0 label 22 19
 2010::/64
  nexthop 2001:8::1 FastEthernet0/0
 2012::/64
  attached to Loopback1
 2012::1/128
  receive
```

Table 98 describes the significant fields shown in the display.

Table 98 show ipv6 cef vrf Field Descriptions

Field	Description
2001:8::/64	Specifies the network prefix.
attached to FastEthernet0/0	Specifies the VRF interface.
nexthop 10.1.1.2 POS4/0 label 22 19	Specifies the BGP next hop address.

show ipv6 cef with epoch

To display Cisco Express Forwarding IPv6 Forwarding Information Base (FIB) information filtered for a specific epoch, use the **show ipv6 cef with epoch** command in privileged EXEC mode.

show ipv6 cef with epoch *epoch-number* [**checksum** | **detail** | **internal** [**checksum**] | **platform** [**checksum** | **detail** | **internal** [**checksum**]]]

Syntax Description

epoch-number	Number of the epoch, from 0 to 255.
checksum	(Optional) Displays FIB entry checksums.
detail	(Optional) Displays detailed information about FIB epochs.
internal	(Optional) Displays internal data structure information.
platform	(Optional) Displays platform-specific data structures.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(25)S	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.
12.2(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 display information about prefix properties for a specified epoch in the Cisco Express Forwarding IPv6 FIB. This command is similar to the **show ip cef with epoch** command, except that it is IPv6 specific. Use the **show ipv6 cef epoch** command to display entries filtered by epoch number.

Examples

The following is sample output from the **show ipv6 cef with epoch** command:

```
Router# show ipv6 cef with epoch 0

::/0
  no route
::/127
  discard
2000::1/128
  receive for Loopback0
2000::2/128
  nexthop FE80::A8BB:CCFF:FE00:2500 Ethernet0/0
2000::3/128
  nexthop FE80::A8BB:CCFF:FE00:2602 Ethernet2/0
2000::4/128
  nexthop FE80::A8BB:CCFF:FE00:2602 Ethernet2/0
2001::/64
```

```
  attached to Ethernet2/0
2001::1/128
  receive for Ethernet2/0
2001::3/128
  attached to Ethernet2/0
2001:1::/64
  attached to Ethernet0/0
2001:1::1/128
  receive for Ethernet0/0
2001:2::/64
  nexthop FE80::A8BB:CCFF:FE00:2602 Ethernet2/0
2002::/64
  attached to Tunnel0
2002::1/128
  receive for Tunnel0
FE80::/10
  receive for Null0
FF00::/8
  receive for Null0
```

Table 99 describes significant fields shown in the display.

Table 99 show ipv6 cef with epoch Field Descriptions

Field	Description
no route	No route is associated with the IPv6 prefix.
discard	Traffic for this prefix is discarded.
2000::1/128 receive for Loopback0	A receive prefix for interface Loopback0.
2000::2/128 nexthop FE80::A8BB:CCFF:FE00:2500 Ethernet0/0	An IPv6 prefix that is forwarded to a next-hop address (FE80::A8BB:CCFF:FE00:2500) through interface Ethernet 0/0.
2001::/64 attached for Ethernet2/0	This prefix is a connected network on interface Ethernet 0/0.
2001::1/128 receive for Ethernet2/0	A receive prefix for interface Ethernet 0/0.

The following is sample output from the **show ipv6 cef with epoch detail** command:

```
Router# show ipv6 cef with epoch 0 detail

IPv6 CEF is enabled and running centrally.
VRF base:
 16 prefixes (16/0 fwd/non-fwd)
 Table id 0
 Database epoch:        0 (16 entries at this epoch)

::/0, epoch 0, flags default route handler
  no route
::/127, epoch 0, flags attached, discard
  discard
2000::1/128, epoch 0, flags attached, connected, receive, local
  receive for Loopback0
2000::2/128, epoch 0
  nexthop FE80::A8BB:CCFF:FE00:2500 Ethernet0/0
2000::3/128, epoch 0, flags rib only nolabel, rib defined all labels
```

```
  nexthop FE80::A8BB:CCFF:FE00:2602 Ethernet2/0
2000::4/128, epoch 0, flags rib only nolabel, rib defined all labels
  nexthop FE80::A8BB:CCFF:FE00:2602 Ethernet2/0
2001::/64, epoch 0, flags attached, connected, cover dependents
  Covered dependent prefixes: 1
    notify cover updated: 1
  attached to Ethernet2/0
2001::1/128, epoch 0, flags attached, receive, local
  receive for Ethernet2/0
2001::3/128, epoch 0, flags attached
  Adj source: IPV6 adj out of Ethernet2/0, addr 2001::3 02513FD8
   Dependent covered prefix type adjfib cover 2001::/64
  attached to Ethernet2/0
2001:1::/64, epoch 0, flags attached, connected
  attached to Ethernet0/0
2001:1::1/128, epoch 0, flags attached, receive, local
  receive for Ethernet0/0
2001:2::/64, epoch 0, flags rib only nolabel, rib defined all labels
  nexthop FE80::A8BB:CCFF:FE00:2602 Ethernet2/0
2002::/64, epoch 0, flags attached, connected
  attached to Tunnel0
2002::1/128, epoch 0, flags attached, receive, local
  receive for Tunnel0
FE80::/10, epoch 0, flags attached, receive, local
  receive for Null0
FF00::/8, epoch 0, flags attached, receive, local
  receive for Null0
```

Table 100 describes significant fields shown in the display.

Table 100 show ipv6 cef with epoch detail Field Descriptions

Field	Description
IPv6 CEF is enabled and running centrally	Indicates that IPv6 CEF is enabled and running on the RP.
VRF base 16 prefixes (16/0 fwd/non-fwd)	Number of prefixes in the VRF, how many of them are forwarded, and how many are not forwarded.
Table id 0	Table identification number.
Database epoch 0 (16 entries at this epoch)	Value of the database epoch and number of entries in the epoch.
2000::1/128, epoch 0, flags attached, connected, receive, local receive for Loopback0	Provides detail for the table entries. In this example, 2000:1/128 is an IPv6 prefix at epoch 0. The flags set for this prefix are: • attached—Prefix is a connected network • connected—Prefix includes an address that is bound to an interface on the device • receive—Prefix is punt to and handled by the process level • local—Prefix is a subset of receive and marks prefixes that are received by on interface on the device

The following is sample output from the **show ipv6 cef with epoch checksum** command:

```
Router# show ipv6 cef with epoch 0 checksum

::/0
  FIB checksum: 0x64E25610
::/127
  FIB checksum: 0xE0B3DE11
2000::1/128
  FIB checksum: 0xD04E36EC
2000::2/128
  FIB checksum: 0x84892BA5
2000::3/128
  FIB checksum: 0x912BA720
2000::4/128
  FIB checksum: 0xC6D89ADA
.
.
.
```

Table 101 describes significant fields shown in the display.

Table 101 show ipv6 cef with epoch checksum Field Descriptions

Field	Description
::/0	Default route handler. ::/0 prefix matches all addresses. (::/128 prefix is an exact match for all zero addresses only.)
FIB checksum: 0x64E25610	FIB checksum associated with the named prefix.

Related Commands

Command	Description
show ip cef with epoch	Displays Cisco Express Forwarding FIB information filtered for a specific epoch.
show ipv6 cef	Displays entries in the IPv6 FIB.
show ipv6 cef epoch	Displays a summary of IPv6 FIB epoch information.

show ipv6 cef with source

To display Cisco Express Forwarding IPv6 Forwarding Information Base (FIB) filtered for a specific source, use the **show ipv6 cef with source** command in privileged EXEC mode.

show ipv6 cef with source *source-type* [**checksum | detail | epoch | internal** [**checksum**] | **platform** [**checksum | detail | internal** [**checksum**]]]

Syntax Description

source-type	The *source-type* argument must be replaced by one of the following keywords that are supported for your release. Keywords for all supported Cisco IOS releases: • **alias**—Displays alias address prefix sources in the Cisco Express Forwarding IPv6 FIB. • **broadband**—Displays broadband receive prefix sources in the Cisco Express Forwarding IPv6 FIB. • **fallback**—Displays fallback lookup prefix sources in the Cisco Express Forwarding IPv6 FIB. • **interface**—Displays interface configuration prefix sources in the Cisco Express Forwarding IPv6 FIB. • **nat**—Displays Network Address Translation (NAT) prefix sources in the Cisco Express Forwarding IPv6 FIB. • **rib**—Displays Routing Information Base (RIB) prefix sources in the Cisco Express Forwarding IPv6 FIB. • **special**—Displays special prefix sources in the Cisco Express Forwarding IPv6 FIB. • **test**—Displays test command prefix sources in the Cisco Express Forwarding IPv6 FIB. • **virtual**—Displays virtual address prefix sources in the Cisco Express Forwarding IPv6 FIB, for example, Virtual Router Redundancy Protocol (VRRP) and Hot Standby Router Protocol (HSRP) addresses. Additional keywords for Cisco IOS Releases 12.2(25)S, 12,2(28)SB, 12.2(33)SRA, and later SB and SR releases: • **adjacency**—Displays adjacency prefix sources in the Cisco Express ForwardingIPv6 FIB. • **default-route**—Displays default route handler prefix sources in the Cisco Express Forwarding FIB. • **inherited-path-list**—Displays inherited path list prefix source in the Cisco Express Forwarding FIB. Additional keywords for Cisco IOS Releases 12.2(33)SXH, 12.4(20)T, and later SX and T releases: • **adj**—Displays adjacency prefix sources in the Cisco Express Forwarding FIB.

	• **defnet—**Displays default network prefix sources in the Cisco Express Forwarding IPv6 FIB. • **defroutehandler**—Displays default route handler prefix sources in the Cisco Express Forwarding IPv6 FIB. • **ipl**—Displays inherited path list prefix source in the Cisco Express ForwardingIPv6 FIB. Additional keywords for Cisco IOS Releases 12.2(33)SRA, 12.2(33)SXH and later SR and SX releases: • **recursive-resolution**—Displays recursive resolution prefix sources in the Cisco Express Forwarding IPv6 FIB. Additional keyword for Cisco IOS Release 12.2(33)SXH and later SX releases: • **lte**—Displays Multiprotocol Label Switching (MPLS) label table entries.
checksum	(Optional) Displays IPv6 FIB entry checksums.
detail	(Optional) Displays detailed information about IPv6 FIB epochs.
epoch	(Optional) Displays information about epochs associated with the source prefix.
internal	(Optional) Displays internal data structure information.
platform	(Optional) Displays platform-specific data structures.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(25)S	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.
12.2(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 filter on prefixes in the Cisco Express Forwarding FIB that are added by a specified source.

Examples

Examples For All Supported Releases

The following is sample output from the **show ipv6 cef with source rib** command:

```
Router# show ipv6 cef with source rib

::/127
  discard
2000::1/128
  receive for Loopback0
2000::2/128
```

```
  nexthop FE80::A8BB:CCFF:FE00:2500 Ethernet0/0
2000::3/128
  nexthop FE80::A8BB:CCFF:FE00:2602 Ethernet2/0
2000::4/128
  nexthop FE80::A8BB:CCFF:FE00:2602 Ethernet2/0
2001::/64
  attached to Ethernet2/0
2001::1/128
  receive for Ethernet2/0
2001:1::/64
  attached to Ethernet0/0
2001:1::1/128
  receive for Ethernet0/0
2001:2::/64
  nexthop FE80::A8BB:CCFF:FE00:2602 Ethernet2/0
2002::/64
  attached to Tunnel0
2002::1/128
  receive for Tunnel0
FE80::/10
  receive for Null0
FF00::/8
  receive for Null0
```

Table 102 describes the significant fields shown in the display.

Table 102 show ipv6 cef with source rib Field Descriptions

Field	Description
::/127	IPv6 prefix.
discard	Indicates that traffic destined for this prefix should be discarded.
2000::1/128 receive for Loopback0	An IPv6 prefix that is a receive prefix for interface Loopback0. Traffic destined for this prefix will be punted to the process level.
2000::2/128 nexthop FE80::A8BB:CCFF:FE00:2500 Ethernet0/0	An IPv6 prefix that is forwarded to a next-hop address (FE80::A8BB:CCFF:FE00:2500) through interface Ethernet 0/0.
2001::/64 attached for Ethernet2/0	An IPv6 prefix that is a connected network on interface Ethernet 0/0. That is, the destination can be reached directly through the specified interface.

The following is sample output from the **show ipv6 cef with source fib detail** command:

```
Router# show ipv6 cef with source rib detail

IPv6 CEF is enabled and running centrally.
VRF base:
 16 prefixes (16/0 fwd/non-fwd)
 Table id 0
 Database epoch:        0 (16 entries at this epoch)

::/127, epoch 0, flags attached, discard
  discard
2000::1/128, epoch 0, flags attached, connected, receive, local
  receive for Loopback0
2000::2/128, epoch 0
  nexthop FE80::A8BB:CCFF:FE00:2500 Ethernet0/0
2000::3/128, epoch 0, flags rib only nolabel, rib defined all labels
```

```
  nexthop FE80::A8BB:CCFF:FE00:2602 Ethernet2/0
2000::4/128, epoch 0, flags rib only nolabel, rib defined all labels
  nexthop FE80::A8BB:CCFF:FE00:2602 Ethernet2/0
2001::/64, epoch 0, flags attached, connected, cover dependents
  Covered dependent prefixes: 1
    notify cover updated: 1
  attached to Ethernet2/0
2001::1/128, epoch 0, flags attached, receive, local
  receive for Ethernet2/0
2001:1::/64, epoch 0, flags attached, connected
  attached to Ethernet0/0
2001:1::1/128, epoch 0, flags attached, receive, local
  receive for Ethernet0/0
2001:2::/64, epoch 0, flags rib only nolabel, rib defined all labels
  nexthop FE80::A8BB:CCFF:FE00:2602 Ethernet2/0
2002::/64, epoch 0, flags attached, connected
  attached to Tunnel0
2002::1/128, epoch 0, flags attached, receive, local
  receive for Tunnel0
FE80::/10, epoch 0, flags attached, receive, local
  receive for Null0
FF00::/8, epoch 0, flags attached, receive, local
  receive for Null0
```

Table 103 describes the significant fields shown in the display.

Table 103 show ipv6 cef with source rib detail Field Descriptions

Field	Description
IPv6 CEF is enabled and running centrally.	Verifies that Cisco Express Forwarding for IPV6 is enabled globally.
VRF base	Base VRF table.
16 prefixes (16/0 Fwd/non-fwd)	Number of prefixes in the VRF, how many prefixes are forwarded, and how many are not forwarded.
Table id 0	Identifies the table by number.
Database epoch:	Specifies the type of epoch.
0 (16 entries at this epoch)	Number of the epoch (0) and number of entries in the epoch.
2000::1/128, epoch 0, flags attached, connected, receive, local	Details about the prefix: the epoch in which it is found, the flags set for the prefix: • attached—Prefix is a connected network • connected—Prefix includes an address that is bound to an interface on the device • receive—Prefix is punt to and handled by the process level • local—Prefix is a subset of receive and marks prefixes that are received by on interface on the device

Examples for Cisco IOS Releases 12.2(25)S, 12.2(28)SB, 12.2(33)SRA, and Later SB and SR Releases

The following is sample output from the **show ipv6 cef with source adjacency** command:

```
Router# show ipv6 cef with source adjacency

2001::3/128
  attached to Ethernet2/0
```

Table 104 describes the significant fields shown in the display.

Table 104 show ipv6 cef with source adjacency Field Descriptions

Field	Description
20001::3/128	IPv6 prefix whose source is an adjacency.
attached to Ethernet2/0	Indicates that the prefix is a connected network through Interface Ethernet 2/0.

The following is sample output from the **show ipv6 cef with source adjacency detail** command:

```
Router# show ipv6 cef with source adjacency detail
#
IPv6 CEF is enabled and running centrally.
VRF Default
 16 prefixes (16/0 fwd/non-fwd)
 Table id 0x1E000000
 Database epoch:        0 (16 entries at this epoch)

2001::3/128, epoch 0, flags attached
  Adj source: IPV6 adj out of Ethernet2/0, addr 2001::3 050878F0
   Dependent covered prefix type adjfib cover 2001::/64
  attached to Ethernet2/0
```

Table 105 describes the significant fields shown in the display.

Table 105 show ipv6 cef with source adjacency detail Field Descriptions

Field	Description
IPv6 CEF is enabled and running centrally.	Verifies that Cisco Express Forwarding for IPV6 is enabled and running on the RP.
VRF Default	Default VRF table.
16 prefixes (16/0 Fwd/non-fwd)	Number of prefixes in the VRF, how many prefixes are forwarded and how many are not forwarded.
Table id 0x1E000000	Identifies the table by hexadecimal number.
2001::3/128, epoch 0, flags attached	Lists a prefix, its epoch number, and flags. Attached flag indicates a connected network.
Adj source: IPv6 adj out of Ethernet2/0, addr 2000::3 050878F0	Indicates that the prefix was sourced by an adjacency and specifies the address family, interface, and address in memory of the adjacency.

Table 105 show ipv6 cef with source adjacency detail Field Descriptions (continued)

Field	Description
Dependent covered prefix type adjfib cover 2001::/64	A prefix sourced by an adjacency is dependent on another less specific prefix (2001::/64) for forwarding information. If this less specific prefix changes, the dependent prefix will need to be recomputed.
attached to Ethernet2/0	Indicates the prefix is a connect network through interface Ethernet 2/0.

The following is sample output from the **show ipv6 cef with source adjacency checksum** command:

```
Router# show ipv6 cef with source adjacency checksum

2001::3/128
  FIB checksum: 0x4AE0F5DC
```

Table 106 describes the significant fields shown in the display.

Table 106 show ipv6 cef with source adjacency checksum Field Descriptions

Field	Description
2001::3/128	IPv6 prefix whose source is an adjacency.
FIB checksum: 0x4AE0F5DC	FIB checksum.

Examples for Cisco IOS Releases 12.2(33)SXH, 12.4(20)T and Later SX and T Releases

The following is sample output from the **show ipv6 cef with source adjacency** command:

```
Router# show ipv6 cef with source adj

2001::3/128
  attached to Ethernet2/0
```

Table 107 describes the significant fields shown in the display.

Table 107 show ipv6 cef with source adj Field Descriptions

Field	Description
20001::3/128	IPv6 prefix whose source is an adjacency.
attached to Ethernet2/0	Indicates that the prefix is a network connected through interface Ethernet 2/0.

The following is sample output from the **show ipv6 cef with source adj detail** command:

```
Router# show ipv6 cef with source adj detail

IPv6 CEF is enabled and running centrally.
VRF base:
 16 prefixes (16/0 fwd/non-fwd)
 Table id 0
 Database epoch:        0 (16 entries at this epoch)

2001::3/128, epoch 0, flags attached
  Adj source: IPV6 adj out of Ethernet2/0, addr 2001::3 02513FD8
```

```
  Dependent covered prefix type adjfib cover 2001::/64
 attached to Ethernet2/0
```

Table 108 describes the significant fields shown in the display.

Table 108 show ipv6 cef with source adj detail Field Descriptions

Field	Description
IPv6 CEF is enabled and running centrally.	Verifies that Cisco Express Forwarding for IPV6 is enabled an running on the RP.
VRF base	Base VRF table.
16 prefixes (16/0 Fwd/non-fwd)	Number of prefixes, and how many prefixes are forwarded and how many are not forwarded.
2001::3/128, epoch 0, flags attached	Provides more detail about the adjacency source, such as epoch number and flags.
Adj source: IPv6 adj out of Ethernet2/0, addr 2000::3 050878F0	Lists a prefix, its epoch number, and flags. Attached flag indicates a connected network.
Dependent covered prefix type adjfib cover 2001::/64	A prefix sourced by an adjacency is dependent on another less specific prefix (2001::/64) for forwarding information. If this less specific prefix changes, the dependent prefix will need to be recomputed.
attached to Ethernet2/0	Indicates the prefix is a connect network through interface Ethernet 2/0.

The following is sample output from the **show ipv6 cef with source adj checksum** command:

```
Router# show ipv6 cef with source adj checksum
2001::3/128
  FIB checksum: 0x4AE0F5DC
```

Table 109 describes the significant fields shown in the display.

Table 109 show ipv6 cef with source adj checksum Field Descriptions

Field	Description
2001::3/128	IPv6 prefix whose source is an adjacency.
FIB checksum: 0x4AE0F5DC	FIB checksum.

Related Commands

Command	Description
show ip cef	Displays entries in the FIB or displays a summary of the FIB.
show ip cef with epoch	Displays information about an epoch in the Cisco Express Forwarding FIB.
show ipv6 cef with epoch	Displays information about an epoch in the Cisco Express Forwarding IPv6 FIB.
show ipv6 cef with source	Displays information about prefix sources in the Cisco Express Forwarding IPv6 FIB.

show ipv6 cga address-db

To display IPv6 cryptographically generated addresses (CGA) from the address database, use the **show ipv6 cga address-db** command in privileged EXEC mode.

show ipv6 cga address-db

Syntax Description

This command has no arguments or keywords.

Command Default

No CGAs are displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(24)T	This command was introduced.

Examples

The following example displays CGAs in the CGA database:

```
Router# show ipv6 cga address-db

2001:0DB8:/64 ::2011:B680:DEF4:A550 - table 0x0
        interface:      Ethernet0/0 (3)
        modifier:       SEND1024e
FE80::/64 ::3824:3CE4:C044:8D65 - table 0x12000003
        interface:      Ethernet0/0 (3)
        modifier:       SEND1024e
```

Table 110 describes the significant fields shown in the display.

Table 110 show ipv6 cga address-db Field Descriptions

Field	Description
2001:0DB8:/64 ::2011:B680:DEF4:A550 - table 0x0	CGA address for which information is shown.
interface:	Interface on which the address is configured.
modifier:	The CGA modifier.

Related Commands

Command	Description
show ipv6 cga modifier-db	Displays IPv6 CGA modifiers.
show ipv6 nd secured certificates	Displays active SeND certificates.
show ipv6 nd secured counters interface	Displays SeND counters on an interface.

Command	Description
show ipv6 nd secured nonce-db	Displays active SeND nonce entries.
show ipv6 nd secured timestamp-db	Displays active SeND time-stamp entries.

show ipv6 cga modifier-db

To display IPv6 cryptographically generated address (CGA) modifier database entries, use the **show ipv6 cga modifier-db** command in privileged EXEC mode.

show ipv6 cga modifier-db

Syntax Description

This command has no arguments or keywords.

Command Default

No CGA modifiers are displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

The **show ipv6 cga modifier-db** command is used to display the modifiers generated with the **ipv6 cga modifier** command and the addresses generated from them.

Examples

The following example displays CGA modifiers in the CGA modifier database:

```
Router# show ipv6 cga modifier-db

F046:E042:13E8:1661:96E5:DD05:94A8:FADC
        label:          SubCA11
        sec level:      1
        Addresses:
       2001:100::38C9:4A1A:2972:794E
       FE80::289C:3308:4719:87F2
```

Table 110 describes the significant fields shown in the display.

Table 111 show ipv6 cga modifier-db Field Descriptions

Field	Description
D695:5D75:F9B5:9715:DF0A:D840:70A2:84B8	The CGA modifier for which the information is displayed.
label	Name used for the Rivest, Shamir, and Adelman (RSA) key pair.
Addresses: 2001:100::38C9:4A1A:2972:794EFE80::289C:3308:4719:87F2	The CGA address.

Related Commands

Command	Description
ipv6 cga modifier	Generates an IPv6 CGA modifier for a specified RSA key pair.
show ipv6 cga address-db	Displays IPv6 CGAs.
show ipv6 nd secured certificates	Displays active SeND certificates.
show ipv6 nd secured counters interface	Displays SeND counters on an interface.
show ipv6 nd secured nonce-db	Displays active SeND nonce entries.
show ipv6 nd secured timestamp-db	Displays active SeND time-stamp entries.

show ipv6 dhcp

To display the Dynamic Host Configuration Protocol (DHCP) unique identifier (DUID) on a specified device, use the **show ipv6 dhcp** command in user EXEC or privileged EXEC mode.

show ipv6 dhcp

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

The **show ipv6 dhcp** command uses the DUID based on the link-layer address for both client and server identifiers. The device uses the MAC address from the lowest-numbered interface to form the DUID. The network interface is assumed to be permanently attached to the device. Use the **show ipv6 dhcp** command to display the DUID of a device.

Examples

The following is sample output from the **show ipv6 dhcp** command. The output is self-explanatory:

```
Router# show ipv6 dhcp

This device's DHCPv6 unique identifier(DUID): 000300010002FCA5DC1C
```

show ipv6 dhcp binding

To display automatic client bindings from the Dynamic Host Configuration Protocol (DHCP) for IPv6 server binding table, use the **show ipv6 dhcp binding** command in user EXEC or privileged EXEC mode.

show ipv6 dhcp binding [*ipv6-address*] [**vrf** *vrf-name*]

Syntax Description

ipv6-address	(Optional) The address of a DHCP for IPv6 client.
vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.4	This command was modified. Command output was updated to display a PPP username associated with a binding.
12.4(24)T	This command was modified. Command output was updated to display address bindings.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.1(2)S	This command was modified. The **vrf** *vrf-name* keyword and argument were added.
Cisco IOS XE Release 3.3S	This command was modified. The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

The **show ipv6 dhcp binding** command displays all automatic client bindings from the DHCP for IPv6 server binding table if the *ipv6-address* argument is not specified. When the *ipv6-address* argument is specified, only the binding for the specified client is displayed.

If the **vrf** *vrf-name* keyword and argument combination is specified, all bindings that belong to the specified VRF are displayed.

Examples

The following sample output displays all automatic client bindings from the DHCP for IPv6 server binding table:

```
Router# show ipv6 dhcp binding

Client: FE80::A8BB:CCFF:FE00:300
  DUID: 00030001AABBCC000300
  Username : client_1
  Interface: Virtual-Access2.1
  IA PD: IA ID 0x000C0001, T1 75, T2 135
    Prefix: 2001:380:E00::/64
```

```
            preferred lifetime 150, valid lifetime 300
            expires at Dec 06 2007 12:57 PM (262 seconds)
Client: FE80::A8BB:CCFF:FE00:300 (Virtual-Access2.2)
  DUID: 00030001AABBCC000300
  IA PD: IA ID 0x000D0001, T1 75, T2 135
    Prefix: 2001:0DB8:E00:1::/64
            preferred lifetime 150, valid lifetime 300
            expires at Dec 06 2007 12:58 PM (288 seconds)
```

Table 112 describes the significant fields shown in the display.

Table 112 show ipv6 dhcp binding Field Descriptions

Field	Description
Client	Address of a specified client.
DUID	DHCP unique identifier (DUID).
Virtual-Access2.1	First virtual client. When an IPv6 DHCP client requests two prefixes with the same DUID but a different identity association for prefix delegation (IAPD) on two different interfaces, these prefixes are considered to be for two different clients, and interface information is maintained for both.
Username : client_1	The username associated with the binding.
IA PD	Collection of prefixes assigned to a client.
IA ID	Identifier for this IAPD.
Prefix	Prefixes delegated to the indicated IAPD on the specified client.
preferred lifetime, valid lifetime	The preferred lifetime and valid lifetime settings, in seconds, for the specified client.
Expires at	Date and time at which the valid lifetime expires.
Virtual-Access2.2	Second virtual client. When an IPv6 DHCP client requests two prefixes with the same DUID but different IAIDs on two different interfaces, these prefixes are considered to be for two different clients, and interface information is maintained for both.

When the DHCPv6 pool on the Cisco IOS DHCPv6 server is configured to obtain prefixes for delegation from an authentication, authorization, and accounting (AAA) server, it sends the PPP username from the incoming PPP session to the AAA server for obtaining the prefixes. The PPP username is associated with the binding is displayed in output from the **show ipv6 dhcp binding** command. If there is no PPP username associated with the binding, this field value is displayed as “unassigned.”

The following example shows that the PPP username associated with the binding is “client_1”:

```
Router# show ipv6 dhcp binding

Client: FE80::2AA:FF:FEBB:CC
  DUID: 0003000100AA00BB00CC
  Username : client_1
  Interface : Virtual-Access2
  IA PD: IA ID 0x00130001, T1 75, T2 135
    Prefix: 2001:0DB8:1:3::/80
            preferred lifetime 150, valid lifetime 300
            expires at Aug 07 2008 05:19 AM (225 seconds)
```

The following example shows that the PPP username associated with the binding is unassigned:

```
Router# show ipv6 dhcp binding

Client: FE80::2AA:FF:FEBB:CC
  DUID: 0003000100AA00BB00CC
  Username : unassigned
  Interface : Virtual-Access2
  IA PD: IA ID 0x00130001, T1 150, T2 240
    Prefix: 2001:0DB8:1:1::/80
            preferred lifetime 300, valid lifetime 300
            expires at Aug 11 2008 06:23 AM (233 seconds)
```

Related Commands

Command	Description
clear ipv6 dhcp binding	Deletes automatic client bindings from the DHCP for IPv6 binding table.

show ipv6 dhcp conflict

To display address conflicts found by a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server when addresses are offered to the client, use the **show ipv6 dhcp conflict** command in privileged EXEC mode.

show ipv6 dhcp conflict [*ipv6-address*] [**vrf** *vrf-name*]

Syntax Description

ipv6-address	(Optional) The address of a DHCP for IPv6 client.
vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(24)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.1(2)S	This command was modified. The **vrf** *vrf-name* keyword and argument were added.
Cisco IOS XE Release 3.3S	This command was modified. The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

When you configure the DHCPv6 server to detect conflicts, it uses ping. The client uses neighbor discovery to detect clients and reports to the server through a DECLINE message. If an address conflict is detected, the address is removed from the pool, and the address is not assigned until the administrator removes the address from the conflict list.

Examples

The following is a sample output from the **show ipv6 dhcp conflict** command. This command shows the pool and prefix values for DHCP conflicts.:

```
Router# show ipv6 dhcp conflict

Pool 350, prefix 2001:0DB8:1005::/48
        2001:0DB8:1005::10
```

Related Commands

Command	Description
clear ipv6 dhcp conflict	Clears an address conflict from the DHCPv6 server database.

show ipv6 dhcp database

To display the Dynamic Host Configuration Protocol (DHCP) for IPv6 binding database agent information, use the **show ipv6 dhcp database** command in user EXEC or privileged EXEC mode.

show ipv6 dhcp database [*agent-URL*]

Syntax Description

agent-URL	(Optional) A flash, NVRAM, FTP, TFTP, or remote copy protocol (RCP) uniform resource locator.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

Each permanent storage to which the binding database is saved is called the database agent. An agent can be configured using the **ipv6 dhcp database** command. Supported database agents include FTP and TFTP servers, RCP, Flash file system, and NVRAM.

The **show ipv6 dhcp database** command displays DHCP for IPv6 binding database agent information. If the *agent-URL* argument is specified, only the specified agent is displayed. If the *agent-URL* argument is not specified, all database agents are shown.

Examples

The following is sample output from the **show ipv6 dhcp database** command:

```
Router# show ipv6 dhcp database

Database agent tftp://172.19.216.133/db.tftp:
  write delay: 69 seconds, transfer timeout: 300 seconds
  last written at Jan 09 2003 01:54 PM,
     write timer expires in 56 seconds
  last read at Jan 06 2003 05:41 PM
  successful read times 1
  failed read times 0
  successful write times 3172
  failed write times 2
Database agent nvram:/dhcpv6-binding:
  write delay: 60 seconds, transfer timeout: 300 seconds
  last written at Jan 09 2003 01:54 PM,
     write timer expires in 37 seconds
  last read at never
  successful read times 0
  failed read times 0
  successful write times 3325
  failed write times 0
Database agent flash:/dhcpv6-db:
```

```
write delay: 82 seconds, transfer timeout: 3 seconds
last written at Jan 09 2003 01:54 PM,
  write timer expires in 50 seconds
last read at never
successful read times 0
failed read times 0
successful write times 2220
failed write times 614
```

Table 113 describes the significant fields shown in the display.

Table 113 show ipv6 dhcp database Field Descriptions

Field	Description
Database agent	Specifies the database agent.
Write delay	The amount of time (in seconds) to wait before updating the database.
transfer timeout	Specifies how long (in seconds) the DHCP server should wait before aborting a database transfer. Transfers that exceed the timeout period are aborted.
Last written	The last date and time bindings were written to the file server.
Write timer expires...	The length of time, in seconds, before the write timer expires.
Last read	The last date and time bindings were read from the file server.
Successful/failed read times	The number of successful or failed read times.
Successful/failed write times	The number of successful or failed write times.

Related Commands

Command	Description
ipv6 dhcp database	Specifies DHCP for IPv6 binding database agent parameters.

show ipv6 dhcp interface

To display Dynamic Host Configuration Protocol (DHCP) for IPv6 interface information, use the **show ipv6 dhcp interface** command in user EXEC or privileged EXEC mode.

show ipv6 dhcp interface [*type number*]

Syntax Description

type number	(Optional) Interface type and number. For more information, use the question mark (**?**) online help function.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.3(11)T	Command output was modified to allow relay agent information to be displayed on a specified interface if the relay agent feature is configured on that interface.
12.4(24)T	Command output was updated to display interface address assignments and T1 and T2 renew/rebind times.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

If no interfaces are specified, all interfaces on which DHCP for IPv6 (client or server) is enabled are shown. If an interface is specified, only information about the specified interface is displayed.

Examples

The following is sample output from the **show ipv6 dhcp interface** command. In the first example, the command is used on a router that has an interface acting as a DHCP for IPv6 server. In the second example, the command is used on a router that has an interface acting as a DHCP for IPv6 client:

```
Router1# show ipv6 dhcp interface

Ethernet2/1 is in server mode
  Using pool: svr-p1
  Preference value: 20
  Rapid-Commit is disabled

Router2# show ipv6 dhcp interface

Ethernet2/1 is in client mode
  State is OPEN (1)
  List of known servers:
```

```
Address: FE80::202:FCFF:FEA1:7439, DUID 000300010002FCA17400
Preference: 20
  IA PD: IA ID 0x00040001, T1 120, T2 192
    Prefix: 3FFE:C00:C18:1::/72
            preferred lifetime 240, valid lifetime 54321
            expires at Nov 08 2002 09:10 AM (54319 seconds)
    Prefix: 3FFE:C00:C18:2::/72
            preferred lifetime 300, valid lifetime 54333
            expires at Nov 08 2002 09:11 AM (54331 seconds)
    Prefix: 3FFE:C00:C18:3::/72
            preferred lifetime 280, valid lifetime 51111
            expires at Nov 08 2002 08:17 AM (51109 seconds)
  DNS server: 1001::1
  DNS server: 1001::2
  Domain name: domain1.net
  Domain name: domain2.net
  Domain name: domain3.net
Prefix name is cli-p1
Rapid-Commit is enabled
```

Table 114 describes the significant fields shown in the display.

Table 114 show ipv6 dhcp interface Field Descriptions

Field	Description
Ethernet2/1 is in server/client mode	Displays whether the specified interface is in server or client mode.
Preference value:	The advertised (or default of 0) preference value for the indicated server.
Prefix name is cli-p1	Displays the IPv6 general prefix pool name, in which prefixes successfully acquired on this interface are stored.
Using pool: svr-p1	The name of the pool that is being used by the interface.
State is OPEN	State of the DHCP for IPv6 client on this interface. “Open” indicates that configuration information has been received.
List of known servers	Lists the servers on the interface.
Address, DUID	Address and DHCP unique identifier (DUID) of a server heard on the specified interface.
Rapid commit is disabled	Displays whether the **rapid-commit** keyword has been enabled on the interface.

The following example shows the DHCP for IPv6 relay agent configuration on FastEthernet interface 0/0, and use of the **show ipv6 dhcp interface** command displays relay agent information on FastEthernet interface 0/0:

```
Router(config-if)# ipv6 dhcp relay destination FE80::250:A2FF:FEBF:A056 FastEthernet0/1

Router# show ipv6 dhcp interface FastEthernet 0/0

FastEthernet0/0 is in relay mode
  Relay destinations:
    FE80::250:A2FF:FEBF:A056 via FastEthernet0/1
```

Related Commands

Command	Description
ipv6 dhcp client pd	Enables the DHCP for IPv6 client process and enables requests for prefix delegation through a specified interface.
ipv6 dhcp relay destination	Specifies a destination address to which client messages are forwarded and enables DHCP for IPv6 relay service on the interface.
ipv6 dhcp server	Enables DHCP for IPv6 service on an interface.

show ipv6 dhcp pool

To display Dynamic Host Configuration Protocol (DHCP) for IPv6 configuration pool information, use the **show ipv6 dhcp pool** command in user EXEC or privileged EXEC mode.

show ipv6 dhcp pool [*poolname*]

Syntax Description

poolname	(Optional) User-defined name for the local prefix pool. The pool name can be a symbolic string (such as "Engineering") or an integer (such as 0).

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.4(24)T	Command output was updated to display address pools and prefix pools.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

Use the **ipv6 dhcp pool** command to create a configuration pool, and use the **ipv6 dhcp server** command to associate the configuration pool with a server on an interface.

The **show ipv6 dhcp pool** command displays DHCP for IPv6 configuration pool information. If the *poolname* argument is specified, only information on the specified pool is displayed. If the *poolname* argument is not specified, information about all pools is shown.

Examples

The following sample output displays DHCP for IPv6 configuration pool information:

```
Router# show ipv6 dhcp pool

DHCPv6 pool: svr-p1
  Static bindings:
    Binding for client 000300010002FCA5C01C
      IA PD: IA ID 00040002,
        Prefix: 3FFE:C00:C18:3::/72
                preferred lifetime 604800, valid lifetime 2592000
      IA PD: IA ID not specified; being used by 00040001
        Prefix: 3FFE:C00:C18:1::/72
                preferred lifetime 240, valid lifetime 54321
        Prefix: 3FFE:C00:C18:2::/72
                preferred lifetime 300, valid lifetime 54333
        Prefix: 3FFE:C00:C18:3::/72
                preferred lifetime 280, valid lifetime 51111
```

```
  Prefix from pool: local-p1, Valid lifetime 12345, Preferred lifetime 180
  DNS server: 1001::1
  DNS server: 1001::2
  Domain name: example1.net
  Domain name: example2.net
  Domain name: example3.net
Active clients: 2
```

Table 115 describes the significant fields shown in the display.

Table 115 show ipv6 dhcp pool Field Descriptions

Field	Description
DHCPv6 pool: svr-p1	The name of the pool.
IA PD	Identity association for prefix delegation (IAPD), which is a collection of prefixes assigned to a client.
IA ID	Identifier for this IAPD.
Prefix	Prefixes to be delegated to the indicated IAPD on the specified client.
preferred lifetime, valid lifetime	Lifetimes, in seconds, associated with the prefix statically assigned to the specified client.
DNS server	IPv6 addresses of the DNS servers.
Domain name	Displays the DNS domain search list.
Active clients	Total number of active clients.

Related Commands

Command	Description
ipv6 dhcp pool	Configures a DHCP for IPv6 configuration information pool and enters DHCP for IPv6 pool configuration mode.
ipv6 dhcp server	Enables DHCP for IPv6 service on an interface.

show ipv6 dhcp relay binding

To display relay bindings from the Dynamic Host Configuration Protocol (DHCP) for IPv6 server binding table, use the **show ipv6 dhcp relay binding** command in user EXEC or privileged EXEC mode.

show ipv6 dhcp relay binding [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.1(2)S	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

If the **vrf** *vrf-name* keyword and argument combination is specified, all bindings belonging to the specified VRF are displayed.

Examples

The following sample allows you to display DHCP for IPv6 relay binding information:

```
Router# show ipv6 dhcp relay binding
```

show ipv6 eigrp events

To display Enhanced Interior Gateway Routing Protocol (EIGRP) events logged for IPv6, use the **show ipv6 eigrp events** command in user EXEC or privileged EXEC mode.

show ipv6 eigrp events [[**errmsg** | **sia**] [*event-num-start event-num-end*] | **type**]

Syntax Description

errmsg	(Optional) Displays error messages being logged.
sia	(Optional) Displays Stuck In Active (SIA) messages.
event-num-start	(Optional) Starting number of the event range. The range is from 1 to 4294967295.
event-num-end	(Optional) Ending number of the event range. The range is from 1 to 4294967295.
type	(Optional) Displays event types being logged.

Command Default

If no event range is specified, information for all IPv6 EIGRP events is displayed.

Command Modes

User EXEC (>)
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) on the Cisco 3845 series routers.

Usage Guidelines

The **show ipv6 eigrp events** command is used to analyze a network failure by the Cisco support team and is not intended for general use. This command provides internal state information about EIGRP and how it processes route notifications and changes.

Examples

The following is sample output from the **show ipv6 eigrp events** command. The fields are self-explanatory.

```
Router# show ipv6 eigrp events

Event information for AS 65535:
1    00:56:41.719 State change: Successor Origin Local origin
2    00:56:41.719 Metric set: 2555:5555::/32 4294967295
3    00:56:41.719 Poison squashed: 2555:5555::/32 lost if
4    00:56:41.719 Poison squashed: 2555:5555::/32 rt gone
5    00:56:41.719 Route installing: 2555:5555::/32 FE80::ABCD:4:EF00:1
6    00:56:41.719 RDB delete: 2555:5555::/32 FE80::ABCD:4:EF00:2
7    00:56:41.719 Send reply: 2555:5555::/32 FE80::ABCD:4:EF00:1
8    00:56:41.719 Find FS: 2555:5555::/32 4294967295
9    00:56:41.719 Free reply status: 2555:5555::/32
10   00:56:41.719 Clr handle num/bits: 0 0x0
11   00:56:41.719 Clr handle dest/cnt: 2555:5555::/32 0
```

```
12   00:56:41.719 Rcv reply met/succ met: 4294967295 4294967295
13   00:56:41.719 Rcv reply dest/nh: 2555:5555::/32 FE80::ABCD:4:EF00:2
14   00:56:41.687 Send reply: 2555:5555::/32 FE80::ABCD:4:EF00:2
15   00:56:41.687 Rcv query met/succ met: 4294967295 4294967295
16   00:56:41.687 Rcv query dest/nh: 2555:5555::/32 FE80::ABCD:4:EF00:2
17   00:56:41.687 State change: Local origin Successor Origin
18   00:56:41.687 Metric set: 2555:5555::/32 4294967295
19   00:56:41.687 Active net/peers: 2555:5555::/32 65536
20   00:56:41.687 FC not sat Dmin/met: 4294967295 2588160
21   00:56:41.687 Find FS: 2555:5555::/32 2588160
22   00:56:41.687 Rcv query met/succ met: 4294967295 4294967295
23   00:56:41.687 Rcv query dest/nh: 2555:5555::/32 FE80::ABCD:4:EF00:1
24   00:56:41.659 Change queue emptied, entries: 1
25   00:56:41.659 Metric set: 2555:5555::/32 2588160
```

Related Commands

Command	Description
clear ipv6 eigrp	Deletes entries from EIGRP for IPv6 routing tables.
debug ipv6 eigrp	Displays information about EIGRP for IPv6 protocol.
ipv6 eigrp	Enables EIGRP for IPv6 on a specified interface.

show ipv6 eigrp interfaces

To display information about interfaces configured for Enhanced Internal Gateway Routing Protocol (EIGRP) for IPv6, use the **show ipv6 eigrp interfaces** command in user EXEC or privileged EXEC mode.

show ipv6 eigrp [*as-number*] **interfaces** [*type number*] [**detail**]

Syntax Description

as-number	(Optional) Autonomous system number.
type	(Optional) Interface type.
number	(Optional) Interface number.
detail	(Optional) Displays detailed interface information.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.4(6)T	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.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

Use the **show ipv6 eigrp interfaces** command to determine on which interfaces EIGRP is active, and to learn information about EIGRP relating to those interfaces. If an interface is specified, only that interface is displayed. Otherwise, all interfaces on which EIGRP is running are displayed.

If an autonomous system is specified, only the routing process for the specified autonomous system is displayed. Otherwise, all EIGRP processes are displayed.

Examples

The following is sample output from the **show ipv6 eigrp interfaces** command:

```
Router# show ipv6 eigrp 1 interfaces

IPv6-EIGRP interfaces for process 1

                     Xmit Queue    Mean    Pacing Time    Multicast     Pending
Interface    Peers   Un/Reliable   SRTT    Un/Reliable    Flow Timer    Routes
Et0/0         0         0/0          0        0/10            0           0
```

The following is sample output from the **show ipv6 eigrp interfaces** command using the **detail** keyword:

```
Router# show ipv6 eigrp interfaces detail

IPv6-EIGRP interfaces for process 1

                     Xmit Queue    Mean    Pacing Time    Multicast    Pending
```

```
Interface    Peers   Un/Reliable   SRTT    Un/Reliable    Flow Timer    Routes
Et0/0          0        0/0           0        0/10            0           0
Hello interval is 5 sec
Next xmit serial <none>
Un/reliable mcasts: 0/0 Un/reliable ucasts: 0/0
Mcast exceptions: 0 CR packets: 0 ACKs suppressed: 0
Retransmissions sent: 0 Out-of-sequence rcvd: 0
Authentication mode is not set
```

Table 116 describes the significant fields shown in the display.

Table 116 show ipv6 eigrp interfaces Field Descriptions

Field	Description
Interface	Interface over which EIGRP is configured.
Peers	Number of directly connected EIGRP neighbors.
Xmit Queue Un/Reliable	Number of packets remaining in the Unreliable and Reliable transmit queues.
Mean SRTT	Mean smooth round-trip time (SRTT) interval (in seconds).
Pacing Time Un/Reliable	Pacing time (in seconds) used to determine when EIGRP packets should be sent out the interface (unreliable and reliable packets).
Multicast Flow Timer	Maximum number of seconds in which the router will send multicast EIGRP packets.
Pending Routes	Number of routes in the packets in the transmit queue waiting to be sent.
Hello interval is 5 sec	Length (in seconds) of the hello interval.

show ipv6 eigrp neighbors

To display the neighbors discovered by Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6, use the **show ipv6 eigrp neighbors** command in user EXEC or privileged EXEC mode.

show ipv6 eigrp neighbors [*interface-type* | *as-number* | **static** | **detail**]

Syntax Description

interface-type	(Optional) Interface type.
as-number	(Optional) Autonomous system number.
static	(Optional) Displays static routes.
detail	(Optional) Displays detailed neighbor information.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.4(6)T	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.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

Use the **show ipv6 eigrp neighbors** command to determine when neighbors become active and inactive. It is also useful for debugging certain types of transport problems.

Examples

The following is sample output from the **show ipv6 eigrp neighbors** command:

```
Router# show ipv6 eigrp neighbors

IPv6-EIGRP neighbors for process 1
H Address                 Interface      Hold      Uptime    SRTT    RTO   Q    Seq
                                         (sec)               (ms)          Cnt  Num
0 Link-local address:         Et0/0         14        00:00:13   11     200   0     2
FE80::A8BB:CCFF:FE00:200
```

Table 116 describes the significant fields shown in the display.

Table 117 show ipv6 eigrp neighbors Field Descriptions

Field	Description
process 1	Autonomous system number.
Address FE80::A8BB:CCFF:FE00:200	IPv6 address of the EIGRP peer.

Table 117 show ipv6 eigrp neighbors Field Descriptions (continued)

Field	Description
Interface	Interface on which the router is receiving hello packets from the peer.
Hold	Length of time (in seconds) that the Cisco IOS software will wait to hear from the peer before declaring it down. If the peer is using the default hold time, this number will be less than 15. If the peer configures a nondefault hold time, the nondefault hold time will be displayed.
Uptime	Elapsed time (in hours:minutes:seconds) since the local router first heard from this neighbor.
SRTT (ms)	Smoothed round-trip time (SRTT). The number of milliseconds required for an EIGRP packet to be sent to this neighbor and for the local router to receive an acknowledgment of that packet.
RTO	Retransmission timeout (in milliseconds). This is the amount of time the software waits before resending a packet from the retransmission queue to a neighbor.
Q count	Number of EIGRP packets (update, query, and reply) that the software is waiting to send.
Seq Num	Sequence number of the last update, query, or reply packet that was received from this neighbor.

The following is sample output from the **show ipv6 eigrp neighbors** command with the **detail** keyword:

```
Router# show ipv6 eigrp neighbors detail

IPv6-EIGRP neighbors for process 1
H  Address                 Interface       Hold      Uptime    SRTT    RTO   Q    Seq
                                           (sec)               (ms)          Cnt  Num
0  Link-local address:        Et0/0         11        00:00:30   11     200   0    2
FE80::A8BB:CCFF:FE00:200
Version 12.4/1.2, Retrans: 0, Retries: 0
```

Table 118 describes the significant fields shown in the display.

Table 118 show ipv6 eigrp neighbors detail Field Descriptions

Field	Description
H	This column lists the order in which a peering session was established with the specified neighbor. The order is specified with sequential numbering starting with 0.
Version	The software version that the specified peer is running.
Retrans	The number of times that a packet has been retransmitted.
Retries	The number of times an attempt was made to retransmit a packet.

The following is sample output from the **show ipv6 eigrp neighbors** command with the **static** keyword:

```
Router# show ipv6 eigrp neighbors static

IPv6-EIGRP neighbors for process 1
Static Address Interface
```

```
Link-local address: Ethernet0/0
FE80::A8BB:CCFF:FE00:200
```

show ipv6 eigrp topology

To display entries in the Enhanced Interior Gateway Routing Protocol (EIGRP) IPv6 topology table, use the **show ipv6 eigrp topology** command in privileged EXEC mode.

show ipv6 eigrp topology [*as-number* | *ipv6-address*] [**active** | **all-links** | **pending** | **summary** | **zero-successors**]

Syntax Description

as-number	(Optional) Autonomous system number.
ipv6-address	(Optional) IPv6 address.
active	(Optional) Displays only active entries in the EIGRP topology table.
all-links	(Optional) Displays all entries in the EIGRP topology table.
pending	(Optional) Displays all entries in the EIGRP topology table that are waiting for an update from a neighbor or are waiting to reply to a neighbor.
summary	(Optional) Displays a summary of the EIGRP topology table.
zero-successors	(Optional) Displays available routes in the EIGRP topology table.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(6)T	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.

Usage Guidelines

The **show ipv6 eigrp topology** command can be used without any keywords or arguments. If this command is used without any keywords or arguments, then only routes that are feasible successors are displayed. The **show ipv6 eigrp topology** command can be used to determine diffusing update algorithm (DUAL) states and to debug possible DUAL problems.

Examples

The following is sample output from the **show ipv6 eigrp topology** command:

```
Router# show ipv6 eigrp topology

IPv6-EIGRP Topology Table for AS(1)/ID(2001:0DB8:10::/64)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r - reply Status, s - sia Status

P 2001:0DB8:3::/64, 1 successors, FD is 281600
via Connected, Ethernet1/0
```

show ipv6 eigrp traffic

To display the number of Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 packets sent and received, use the **show ipv6 eigrp traffic** command in user EXEC or privileged EXEC mode.

show ipv6 eigrp traffic [*as-number*]

Syntax Description

as-number	(Optional) Autonomous system number.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.4(6)T	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.

Usage Guidelines

Use the **show ipv6 eigrp traffic** command to provide information on packets received and sent.

Examples

The following is sample output from the **show ipv6 eigrp traffic** command:

```
Router# show ipv6 eigrp traffic

IPv6-EIGRP Traffic Statistics for process 9
 Hellos sent/received: 218/205
 Updates sent/received: 7/23
 Queries sent/received: 2/0
 Replies sent/received: 0/2
 Acks sent/received: 21/14
```

Table 167 describes the significant fields shown in the display.

Table 167 show ipv6 eigrp traffic Field Descriptions

Field	Description
process 9	Autonomous system number specified in the **ipv6 router eigrp** command.
Hellos sent/received	Number of hello packets sent and received.
Updates sent/received	Number of update packets sent and received.
Queries sent/received	Number of query packets sent and received.
Replies sent/received	Number of reply packets sent and received.
Acks sent/received	Number of acknowledgment packets sent and received.

Related Commands

Command	Description
ipv6 router eigrp	Configures the EIGRP for IPv6 routing process.

show ipv6 flow cache aggregation

To display the aggregation cache configuration, use the **show ipv6 cache flow aggregation** command in privileged EXEC mode.

show ipv6 flow cache aggregation *aggregation-type* [**verbose**]

Syntax Description

aggregation-type	Displays the configuration of a particular aggregation cache as follows: • Autonomous system • Destination prefix • Prefix • Protocol-port • Source prefix
verbose	(Optional) Displays additional information from the aggregation cache.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)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.

Examples

The following is an example display of an autonomous system aggregation cache using the **show iv6 flow cache aggregation as** command:

```
Router# show ipv6 flow cache aggregation as

IPv6 Flow Switching Cache, 278544 bytes
  2 active, 4094 inactive, 13 added
  178 ager polls, 0 flow alloc failures

Src If       Src AS  Dst If       Dst AS  Flows   Pkts  B/Pk  Active
Fa1/0         0      Null          0         1      2     49    10.2
Fa1/0         0      Se2/0         20        1      5    100     0.0
```

The following is a sample display of an autonomous system aggregation cache for the prefix mask 2001::FFFC/64 using the **show ipv6 flow cache aggregation as** command:

```
Router# show ipv6 flow cache aggregation as

IPv6 Flow Switching Cache, 278544 bytes
  2 active, 4094 inactive, 13 added
  178 ager polls, 0 flow alloc failures

Src If         Src AS  Dst If         Dst AS     Flows    Pkts  B/Pk  Active
e1/2            0      Null            0            1     2       49    10.2
e1/2            0      e1/2           20            1     5      100     0.0
```

The following is a sample display of an autonomous system aggregation cache for Ethernet1/2 using the **show ipv6 flow cache verbose aggregation as** command:

```
Router# show ipv6 flow cache aggregation as verbose

IPv6 Flow Switching Cache, 278544 bytes
  2 active, 4094 inactive, 13 added
  178 ager polls, 0 flow alloc failures

Src If         Src AS  Dst If         Dst AS     Flows    Pkts  B/Pk  Active
e1/2            0      Null            0            1     2       49    10.2
e1/2            0      e1/2           20            1     5      100     0.0
```

Table 168 describes the significant fields shown in these examples.

Table 168 show ipv6 flow cache aggregation Field Descriptions

Field	Description
bytes	Number of bytes of memory used by the NetFlow cache.
active	Number of active flows in the NetFlow cache at the time this command was entered.
inactive	Number of flow buffers that are allocated in the NetFlow cache, but are not currently assigned to a specific flow at the time this command is entered.
added	Number of flows created since the start of the summary period.
ager polls	Number of times the NetFlow code looked at the cache to cause entries to expire (used by Cisco for diagnostics only).
flow alloc failures	Number of times the NetFlow code tried to allocate a flow but could not.
Src If	Specifies the source interface.
Src AS	Specifies the source autonomous system.
Dst If	Specifies the destination interface.
Dst AS	Specifies the destination autonomous system.
Flows	Number of flows.
Pkts	Number of packets.
B/Pk	Average number of bytes observed for the packets seen for this protocol (total bytes for this protocol or the total number of flows for this protocol for this summary period).
Active	Number of active flows in the NetFlow cache at the time this command was entered.

Related Commands

Command	Description
ipv6 flow-aggregation cache	Enables aggregation cache configuration mode.

show ipv6 flow export

To display the statistics for the data export, including the main cache and all other enabled caches, use the **showipv6 flow export** command in user EXEC or privileged EXEC mode.

show ipv6 flow export [**template**]

Syntax Description

template	(Optional) Displays export template statistics.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)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.

Examples

The following is sample output from the **show ipv6 flow export** command:

```
Router# show ipv6 flow export

Flow export is enabled
   Exporting flows to 10.42.42.1 (9991) 10.0.101.254 (9991)
   Exporting using source IP address 10.0.101.203
   Version 5 flow records
   Export Stats for 10.42.42.1 (9991)
           3 flows exported in 3 udp datagrams
           0 flows failed due to lack of export packet
           3 export packets were sent up to process level
           0 export packets were dropped due to no fib
           0 export packets were dropped due to adjacency issues
           0 export packets were dropped enqueuing for the RP
           0 export packets were dropped due to IPC rate limiting
   Export Stats for 10.0.101.254 (9991)
           7 flows exported in 7 udp datagrams
           0 flows failed due to lack of export packet
           6 export packets were sent up to process level
           0 export packets were dropped due to no fib
           0 export packets were dropped due to adjacency issues
           0 export packets were dropped enqueuing for the RP
           0 export packets were dropped due to IPC rate limiting
```

Table 169 describes the significant fields shown in the display.

Table 169 show ipv6 flow export Field Descriptions

Field	Description
Exporting flows to 10.42.42.1 (9991) 10.0.101.254 (9991)	Specifies the export destinations and ports. The ports are in parentheses.
Exporting using source IP address 10.0.101.203	Specifies the source address or interface.
Version 5 flow records	Specifies the version of the flow.
3 flows exported in 3udp datagrams	The total number of export packets sent, and the total number of flows contained within them.
0 flows failed due to lack of export packet	No memory was available to create an export packet.
0 export packets were sent up to process level	The packet could not be processed by CEF or by fast switching, possibly because another feature requires running on the packet.
0 export packets were dropped due to no fib 0 export packets were dropped due to adjacency issues	Indicates that CEF was unable to switch the packet or forward it up to the process level.
0 export packets were dropped enqueuing for the RP 0 export packets were dropped due to IPC rate limiting	Indicates that there was a problem transferring the export packet between the RP and the line card.

show ipv6 general-prefix

To display information on IPv6 general prefixes, use the **show ipv6 general-prefix** command in user EXEC or privileged EXEC mode.

show ipv6 general-prefix

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

Use the **show ipv6 general-prefix** command to view information on IPv6 general prefixes.

Examples

The following example shows an IPv6 general prefix called my-prefix, which has been defined based on a 6to4 interface. The general prefix is also being used to define an address on interface loopback42.

```
Router# show ipv6 general-prefix

IPv6 Prefix my-prefix, acquired via 6to4
2002:B0B:B0B::/48
 Loopback42 (Address command)
```

Table 170 describes the significant fields shown in the display.

Table 170 show ipv6 general-prefix Field Descriptions

Field	Description
IPv6 Prefix	User-defined name of the IPv6 general prefix.
Acquired via	The general prefix has been defined based on a 6to4 interface. A general prefix can also be defined manually or acquired using DHCP for IPv6 prefix delegation.
2002:B0B:B0B::/48	The prefix value for this general prefix.
Loopback42 (Address command)	List of interfaces where this general prefix is used.

Related Commands

Command	Description
ipv6 general-prefix	Defines a general prefix for an IPv6 address manually.

show ipv6 inspect

To view Context-based Access Control (CBAC) configuration and session information, use the **show ipv6 inspect** command in privileged EXEC mode.

show ipv6 inspect {**name** *inspection-name* | **config** | **interfaces** | **session** [**detail**] | **all**}

Syntax Description

name *inspection-name*	Displays the configured inspection rule with the name *inspection-name*.
config	Displays the complete Cisco IOS firewall inspection configuration.
interfaces	Displays interface configuration with respect to applied inspection rules and access lists.
session [**detail**]	Displays existing sessions that are currently being tracked and inspected by Cisco IOS firewall. The optional **detail** keyword causes additional details about these sessions to be shown.
all	Displays all Cisco IOS firewall configuration and all existing sessions that are currently being tracked and inspected by Cisco IOS firewall.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(7)T	This command was introduced.

Examples

The following example asks for information about interfaces currently under inspection:

```
Router# show ipv6 inspect interfaces
```

Related Commands

Command	Description
ipv6 inspect	Applies a set of inspection rules to an interface.

show ipv6 interface

To display the usability status of interfaces configured for IPv6, use the **show ipv6 interface** command in user EXEC or privileged EXEC mode.

show ipv6 interface [**brief**] [*type number*] [**prefix**]

Syntax Description

brief	(Optional) Displays a brief summary of IPv6 status and configuration for each interface.
type	(Optional) The interface type about which to display information.
number	(Optional) The interface number about which to display information.
prefix	(Optional) Prefix generated from a local IPv6 prefix pool.

Command Default

All IPv6 interfaces are displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(4)T	The OK, TENTATIVE, DUPLICATE, ICMP redirects, and ND DAD fields were added to the command output.
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 Release 12.2(14)S.
12.2(25)S	Command output was updated to display information on the current Unicast RPF configuration.
12.4(2)T	Command output was updated to show the state of the default router preference (DRP) preference value as advertised by a router through an interface.
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.
12.4(4)T	Command output was updated to show Hot Standby Router Protocol (HSRP) for IPv6 information.
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 introduced on Cisco ASR 1000 series routers.
12.4(24)T	Command output was updated to show the Dynamic Host Configuration Protocol (DHCP) originated addresses.

Usage Guidelines

The **show ipv6 interface** command provides output similar to the **show ip interface** command, except that it is IPv6-specific.

Use the **show ipv6 interface** command to validate the IPv6 status of an interface and its configured addresses. The **show ipv6 interface** command also displays the parameters that IPv6 is using for operation on this interface and any configured features.

If the interface's hardware is usable, the interface is marked up. If the interface can provide two-way communication for IPv6, the line protocol is marked up.

If you specify an optional interface type and number, the command displays information only about that specific interface. For a specific interface, you can enter the **prefix** keyword to see the IPv6 neighbor discovery (ND) prefixes that are configured on the interface.

Examples

Interface Information for a Specific Interface with IPv6 Configured

The **show ipv6 interface** command displays information about the specified interface.

```
Router# show ipv6 interface ethernet 0/0

Ethernet0 is up, line protocol is up
  IPv6 is enabled, link-local address is 2001:0DB8::/29
  Global unicast address(es):
    2000:0DB8::2, subnet is 2001:0DB8::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF11:6770
  MTU is 1500 bytes
  ICMP error messages limited to one every 500 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
```

Table 171 describes the significant fields shown in the display.

Table 171 show ipv6 interface Field Descriptions

Field	Description
Ethernet 0 is up, down, administratively down (down and administratively down are not shown in sample output)	Indicates whether the interface hardware is active (whether line signal is present) and whether it has been taken down by an administrator. If the interface hardware is usable, the interface is marked "up." For an interface to be usable, both the interface hardware and line protocol must be up.
line protocol is up, down (down is not shown in sample output)	Indicates whether the software processes that handle the line protocol consider the line usable (that is, whether keepalives are successful or IPv6 CP has been negotiated). If the interface can provide two-way communication, the line protocol is marked up. For an interface to be usable, both the interface hardware and line protocol must be up.

Table 171 show ipv6 interface Field Descriptions (continued)

Field	Description
IPv6 is enabled, stalled, disabled (stalled and disabled are not shown in sample output)	Indicates that IPv6 is enabled, stalled, or disabled on the interface. If IPv6 is enabled, the interface is marked "enabled." If duplicate address detection processing identified the link-local address of the interface as being a duplicate address, the processing of IPv6 packets is disabled on the interface and the interface is marked "stalled." If IPv6 is not enabled, the interface is marked "disabled."
link-local address	Displays the link-local address assigned to the interface.
Global unicast address(es):	Displays the global unicast addresses assigned to the interface.
Joined group address(es):	Indicates the multicast groups to which this interface belongs.
MTU	Maximum transmission unit of the interface.
ICMP error messages	Specifies the minimum interval (in milliseconds) between error messages sent on this interface.
ICMP redirects	The state of Internet Control Message Protocol (ICMP) IPv6 redirect messages on the interface (the sending of the messages is enabled or disabled).
ND DAD	The state of duplicate address detection on the interface (enabled or disabled).
number of DAD attempts:	Number of consecutive neighbor solicitation messages that are sent on the interface while duplicate address detection is performed.
ND reachable time	Displays the neighbor discovery reachable time (in milliseconds) assigned to this interface.
ND advertised reachable time	Displays the neighbor discovery reachable time (in milliseconds) advertised on this interface.
ND advertised retransmit interval	Displays the neighbor discovery retransmit interval (in milliseconds) advertised on this interface.
ND router advertisements	Specifies the interval (in seconds) for neighbor discovery router advertisements sent on this interface and the amount of time before the advertisements expire. As of Cisco IOS Release 12.4(2)T, this field displays the default router preference (DRP) value sent by this router on this interface.
ND advertised default router preference is Medium	The DRP for the router on a specific interface.

show ipv6 interface Command Using the brief Keyword

The following is sample output from the **show ipv6 interface** command when entered with the **brief** keyword:

```
Router# show ipv6 interface brief

Ethernet0 is up, line protocol is up
Ethernet0                  [up/up]
    unassigned
```

```
Ethernet1                  [up/up]
    2001:0DB8:1000:/29
Ethernet2                  [up/up]
    2001:0DB8:2000:/29
Ethernet3                  [up/up]
    2001:0DB8:3000:/29
Ethernet4                  [up/down]
    2001:0DB8:4000:/29
Ethernet5                  [administratively down/down]
    2001:123::210:7BFF:FEC2:ACD8

Interface         Status                IPv6 Address
Ethernet0         up                    3FFE:C00:0:1:260:3EFF:FE11:6770
Ethernet1         up                    unassigned
Fddi0             up                    3FFE:C00:0:2:260:3EFF:FE11:6772
Serial0           administratively down unassigned
Serial1           administratively down unassigned
Serial2           administratively down unassigned
Serial3           administratively down unassigned
Tunnel0           up                    unnumbered (Ethernet0)
Tunnel1           up                    3FFE:700:20:1::12
```

IPv6 Interface with ND Prefix Configured

This sample output shows the characteristics of an interface that has generated a prefix from a local IPv6 prefix pool:

```
Router# show ipv6 interface Ethernet 0/0 prefix

interface Ethernet0/0
 ipv6 address 2001:0DB8::1/64
 ipv6 address 2001:0DB8::2/64
 ipv6 nd prefix 2001:0DB8:2::/64
 ipv6 nd prefix 2001:0DB8:3::/64 2592000 604800 off-link
end
.
.
.
IPv6 Prefix Advertisements Ethernet0/0
Codes: A - Address, P - Prefix-Advertisement, O - Pool
       U - Per-user prefix, D - Default
       N - Not advertised, C - Calendar

     default [LA] Valid lifetime 2592000, preferred lifetime 604800
AD   2001:0DB8:1::/64 [LA] Valid lifetime 2592000, preferred lifetime 604800
APD  2001:0DB8:2::/64 [LA] Valid lifetime 2592000, preferred lifetime 604800
P    2001:0DB8:3::/64 [A] Valid lifetime 2592000, preferred lifetime 604800
```

The default prefix shows the parameters that are configured using the **ipv6 nd prefix default** command.

IPv6 Interface with DRP Configured

This sample output shows the state of the DRP preference value as advertised by this router through an interface:

```
Router# show ipv6 interface gigabitethernet 0/1

  GigabitEthernet0/1 is up, line protocol is up
    IPv6 is enabled, link-local address is FE80::130
    Description: Management network (dual stack)
    Global unicast address(es):
      FEC0:240:104:1000::130, subnet is FEC0:240:104:1000::/64
    Joined group address(es):
      FF02::1
```

```
    FF02::2
    FF02::1:FF00:130
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Low
  Hosts use stateless autoconfig for addresses.
```

IPv6 Interface with HSRP Configured

When HSRP IPv6 is first configured on an interface, the interface IPv6 link-local address is marked unactive (UNA) because it is no longer advertised, and the HSRP IPv6 virtual link-local address is added to the virtual link-local address list with the UNA and tentative DAD (TEN) flags set. The interface is also programmed to listen for the HSRP IPv6 multicast address.

This sample output shows the status of UNA and TEN flags, when HSRP IPv6 is configured on an interface:

```
Router# show ipv6 interface ethernet 0/0

Ethernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80:2::2 [UNA]
  Virtual link-local address(es):
    FE80::205:73FF:FEA0:1 [UNA/TEN]
  Global unicast address(es):
    2001:2::2, subnet is 2001:2::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::66
    FF02::1:FF00:2
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ND DAD is enabled, number of DAD attempts: 1
```

After the HSRP group becomes active, the UNA and TEN flags are cleared, and the optimistic DAD (OPT) flag is set. The solicited node multicast address for the HSRP virtual IPv6 address is also added to the interface.

This sample output shows the status of UNA, TEN and OPT flags, when HSRP group is activated:

```
Router# show ipv6 interface ethernet 0/0

Ethernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80:2::2 [UNA]
  Virtual link-local address(es):
    FE80::205:73FF:FEA0:1 [OPT]
  Global unicast address(es):
    2001:2::2, subnet is 2001:2::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::66
    FF02::1:FF00:2
    FF02::1:FFA0:1
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
```

Table 172 describes additional significant fields shown in the displays for the **show ipv6 interface** command with HSRP configured.

Table 172 show ipv6 interface Command with HSRP Configured Field Descriptions

Field	Description
IPv6 is enabled, link-local address is FE80:2::2 [UNA]	The interface IPv6 link-local address is marked UNA because it is no longer advertised.
FE80::205:73FF:FEA0:1 [UNA/TEN]	The virtual link-local address list with the UNA and TEN flags set.
FF02::66	HSRP IPv6 multicast address.
FE80::205:73FF:FEA0:1 [OPT]	HSRP becomes active, and the HSRP virtual address marked OPT.
FF02::1:FFA0:1	HSRP solicited node multicast address.

IPv6 Interface with Minimum RA Interval Configured

When you enable Mobile IPv6 on an interface, you can configure a minimum interval between IPv6 router advertisement (RA) transmissions. The **show ipv6 interface** command output reports the minimum RA interval, when configured. If the minimum RA interval is not explicitly configured, then it is not displayed.

In the following example, the maximum RA interval is configured as 100 seconds, and the minimum RA interval is configured as 60 seconds on Ethernet interface 1/0:

```
Router(config-if)# ipv6 nd ra-interval 100 60
```

Subsequent use of the **show ipv6 interface** then displays the interval as follows:

```
Router(config)# show ipv6 interface ethernet 1/0

Ethernet1/0 is administratively down, line protocol is down
  IPv6 is enabled, link-local address is FE80::A8BB:CCFF:FE00:5A01 [TEN]
  No Virtual link-local address(es):
  No global unicast address is configured
  Joined group address(es):
    FF02::1
    FF02::2
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 60 to 100 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
```

In the following example, the maximum RA interval is configured as 100 milliseconds (ms), and the minimum RA interval is configured as 60 ms on Ethernet interface 1/0:

```
Router(config)# show ipv6 interface ethernet 1/0

Ethernet1/0 is administratively down, line protocol is down
```

```
IPv6 is enabled, link-local address is FE80::A8BB:CCFF:FE00:5A01 [TEN]
No Virtual link-local address(es):
No global unicast address is configured
Joined group address(es):
  FF02::1
  FF02::2
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP unreachables are sent
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 60 to 100 milliseconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Hosts use stateless autoconfig for addresses.
```

Table 173 describes additional significant fields shown in the displays for the **show ipv6 interface** command with minimum RA interval information configured.

Table 173 show ipv6 interface Command with Minimum RA Interval Information Configuration Field Descriptions

Field	Description
ND router advertisements are sent every 60 to 100 seconds	ND RAs are sent at an interval randomly selected from a value between the minimum and maximum values. In this example, the minimum value is 60 seconds, and the maximum value is 100 seconds.
ND router advertisements are sent every 60 to 100 milliseconds	ND RAs are sent at an interval randomly selected from a value between the minimum and maximum values. In this example, the minimum value is 60 ms, and the maximum value is 100 ms.

Related Commands

Command	Description
ipv6 nd prefix	Configures which IPv6 prefixes are included in IPv6 router advertisements.
ipv6 nd ra interval	Configures the interval between IPv6 RA transmissions on an interface.
show ip interface	Displays the usability status of interfaces configured for IP.

show ipv6 local pool

To display information about any defined IPv6 address pools, use the **show ipv6 local pool** command in privileged EXEC mode.

show ipv6 local pool [*poolname* [**cache**]]

Syntax Description

poolname	(Optional) User-defined name for the local address pool.
cache	(Optional) Indicates that cache statistics are to be included in the output display

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

If you omit the *poolname* argument, the command displays a generic list of all defined address pools and the IP addresses that belong to them. If you specify the *poolname* argument, the command displays detailed information about that pool.

Examples

The following command displays IPv6 prefix pool information, which includes cache statistics:

```
Router# show ipv6 local pool mypool

Prefix is 2001:0DB8::/29 assign /64 prefix
2 entries in use, 254 available, 0 rejected
0 entries cached, 1000 maximum

User           Prefix               Interface
joe            3FFE:FFFF:A::/64      Vi1
john           3FFE:FFFF:A:1::/64    Vi2
```

The following command displays IPv6 prefix pool information for all prefix pools:

```
Router# show ipv6 local pool

Pool Prefix Free In use
mypool 2001:0DB8::/29 65516 20
myrouter#
myrouter# show ipv6 local pool mypool
Prefix is 1234::/48 assign /64 prefix
20 entries in use, 65516 available, 0 rejected
0 entries cached, 1000 maximum
User Prefix Interface
user1-72b 1234::/64 Vi1.21
user1-72b 1234:0:0:1::/64 Vi1.22
user1-72b 1234:0:0:2::/64 Vi1.23
user1-72b 1234:0:0:3::/64 Vi1.24
user1-72b 1234:0:0:4::/64 Vi1.25
user1-72b 1234:0:0:5::/64 Vi1.26
```

```
user1-72b 1234:0:0:6::/64 Vi1.27
user1-72b 1234:0:0:7::/64 Vi1.28
user1-72b 1234:0:0:8::/64 Vi1.29
user1-72b 1234:0:0:9::/64 Vi1.30
user1-72b 1234:0:0:A::/64 Vi1.31
user1-72b 1234:0:0:B::/64 Vi1.32
user1-72b 1234:0:0:C::/64 Vi1.33
user1-72b 1234:0:0:D::/64 Vi1.34
user1-72b 1234:0:0:E::/64 Vi1.35
user1-72b 1234:0:0:F::/64 Vi1.36
user1-72b 1234:0:0:10::/64 Vi1.37
user1-72b 1234:0:0:11::/64 Vi1.38
user1-72b 1234:0:0:12::/64 Vi1.39
user1-72b 1234:0:0:13::/64 Vi1.40
```

Table 174 describes the significant fields shown in the displays.

Table 174 show ipv6 local pool Field Descriptions

Field	Description
Scope	The type of access.
Pool	Pool and group names and associations, if created.
Begin	The first IP address in the defined range of addresses in this pool.
End	The last IP address in the defined range of addresses in this pool.
Free	The number of addresses available.
InUse	The number of addresses in use.

Related Commands

Command	Description
ipv6 local pool	Configures a local pool of IPv6 addresses to be used when a remote peer connects to a point-to-point interface.

show ipv6 mfib

To display the forwarding entries and interfaces in the IPv6 Multicast Forwarding Information Base (MFIB), use the **show ipv6 mfib** command in user EXEC or privileged EXEC mode.

Cisco 3660 Series Routers, Cisco 10000 Series Routers, and Catalyst 6500 Series Routers

show ipv6 mfib [**vrf** *vrf-name*] [**all** | **linkscope** | **verbose** | *group-address-name* | *ipv6-prefix*/*prefix-length* | *source-address-name* | **interface** | **status** | **summary**]

Cisco 7600 Series Routers

show ipv6 mfib [**vrf** *vrf-name*] [**all** | **linkscope** | **verbose** | **interface** | **status** | **summary**]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
all	(Optional) Displays all forwarding entries and interfaces in the IPv6 MFIB.
linkscope	(Optional) Displays the link-local groups.
verbose	(Optional) Provides additional information, such as the MAC encapsulation header and platform-specific information.
ipv6-prefix	(Optional) The IPv6 network assigned to the interface. The default IPv6 prefix is 128. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/prefix-length	(Optional) The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
group-address-name	(Optional) IPv6 address or name of the multicast group.
source-address-name	(Optional) IPv6 address or name of the multicast group.
interface	(Optional) Interface settings and status.
status	(Optional) General settings and status.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	The **link-local** keyword was added.
12.2(18)SXE	Support for this command was added for the Supervisor Engine 720.
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.
12.3(4)T	The **link-local** keyword was added.

Release	Modification
12.3(7)T	The *ipv6-prefix* and *prefix-length* arguments were 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.
15.0(1)M	This command was modified. The **link-local** keyword was changed to **linkscope**.
Cisco IOS Release 15.1(1)S	This command was modified. New counters were added to the output to show (*,G/m) and the total number of unique groups in the database.
Cisco IOS XE Release 3.2S	This command was modified. New counters were added to the output to show (*,G/m) and the total number of unique groups in the database.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

Use the **show ipv6 mfib** command to display MFIB entries; and forwarding interfaces, and their traffic statistics. This command can be enabled on virtual IP (VIP) if the router is operating in distributed mode.

A forwarding entry in the MFIB has flags that determine the default forwarding and signaling behavior to use for packets matching the entry. The entry also has per-interface flags that further specify the forwarding behavior for packets received or forwarded on specific interfaces. Table 175 describes the MFIB forwarding entries and interface flags.

Table 175 MFIB Entries and Interface Flags

Flag	Description
F	Forward—Data is forwarded out of this interface.
A	Accept—Data received on this interface is accepted for forwarding.
IC	Internal copy—Deliver to the router a copy of the packets received or forwarded on this interface.
NS	Negate signal—Reverse the default entry signaling behavior for packets received on this interface.
DP	Do not preserve—When signaling the reception of a packet on this interface, do not preserve a copy of it (discard it instead).
SP	Signal present—The reception of a packet on this interface was just signaled.
S	Signal—By default, signal the reception of packets matching this entry.
C	Perform directly connected check for packets matching this entry. Signal the reception if packets were originated by a directly connected source.

Examples

The following example displays the forwarding entries and interfaces in the MFIB. The router is configured for fast switching, and it has a receiver joined to FF05::1 on Ethernet1/1 and a source (2001::1:1:20) sending on Ethernet1/2:

```
Router# show ipv6 mfib

IP Multicast Forwarding Information Base
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
```

```
Other counts: Total/RPF failed/Other drops
Interface Flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,FF00::/8) Flags: C
   Forwarding: 0/0/0/0, Other: 0/0/0
   Tunnel0 Flags: NS
(*,FF00::/15) Flags: D
   Forwarding: 0/0/0/0, Other: 0/0/0
(*,FF05::1) Flags: C
   Forwarding: 2/0/100/0, Other: 0/0/0
   Tunnel0 Flags: A NS
   Ethernet1/1 Flags: F NS
     Pkts: 0/2
(2001::1:1:200,FF05::1) Flags:
   Forwarding: 5/0/100/0, Other: 0/0/0
   Ethernet1/2 Flags: A
   Ethernet1/1 Flags: F NS
     Pkts: 3/2
(*,FF10::/15) Flags: D
   Forwarding: 0/0/0/0, Other: 0/0/0
```

Table 176 describes the significant fields shown in the display.

Table 176 show ipv6 mfib Field Descriptions

Field	Description
Entry Flags	Information about the entry.
Forwarding Counts	Statistics on the packets that are received from and forwarded to at least one interface.
Pkt Count/	Total number of packets received and forwarded since the creation of the multicast forwarding state to which this counter applies.
Pkts per second/	Number of packets received and forwarded per second.
Avg Pkt Size/	Total number of bytes divided by the total number of packets for this multicast forwarding state. There is no direct display for the total number of bytes. You can calculate the total number of bytes by multiplying the average packet size by the packet count.
Kbits per second	Bytes per second divided by packets per second divided by 1000.
Other counts:	Statistics on the received packets. These counters include statistics about the packets received and forwarded and packets received but not forwarded.
Interface Flags:	Information about the interface. See Table 175 for further information on interface flags.
Interface Counts:	Interface statistics.

The following example shows forwarding entries and interfaces in the MFIB, with a group address of FF03:1::1 specified:

```
Router# show ipv6 mfib FF03:1::1

IP Multicast Forwarding Information Base
Entry Flags:C - Directly Connected, S - Signal, IA - Inherit A
flag,
            AR - Activity Required, D - Drop
Forwarding Counts:Pkt Count/Pkts per second/Avg Pkt Size/Kbits per
```

```
second
Other counts:Total/RPF failed/Other drops
Interface Flags:A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts:FS Pkt Count/PS Pkt Count
*,FF03:1::1) Flags:C
  Forwarding:0/0/0/0, Other:0/0/0
  Tunnel1 Flags:A NS
  GigabitEthernet5/0.25 Flags:F NS
    Pkts:0/0
  GigabitEthernet5/0.24 Flags:F NS
    Pkts:0/0
(5002:1::2,FF03:1::1) Flags:
  Forwarding:71505/0/50/0, Other:42/0/42
  GigabitEthernet5/0 Flags:A
  GigabitEthernet5/0.19 Flags:F NS
    Pkts:239/24
  GigabitEthernet5/0.20 Flags:F NS
    Pkts:239/24
  GigabitEthernet5/0.21 Flags:F NS
    Pkts:238/24
.
.
.
GigabitEthernet5/0.16 Flags:F NS
Pkts:71628/24
```

The following example shows forwarding entries and interfaces in the MFIB, with a group address of FF03:1::1 and a source address of 5002:1::2 specified:

```
Router# show ipv6 mfib FF03:1::1 5002:1::2

IP Multicast Forwarding Information Base
Entry Flags:C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop
Forwarding Counts:Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts:Total/RPF failed/Other drops
Interface Flags:A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts:FS Pkt Count/PS Pkt Count
(5002:1::2,FF03:1::1) Flags:
   Forwarding:71505/0/50/0, Other:42/0/42
   GigabitEthernet5/0 Flags:A
   GigabitEthernet5/0.19 Flags:F NS
     Pkts:239/24
   GigabitEthernet5/0.20 Flags:F NS
     Pkts:239/24
.
.
.
   GigabitEthernet5/0.16 Flags:F NS
     Pkts:71628/24
```

The following example shows forwarding entries and interfaces in the MFIB, with a group address of FF03:1::1 and a default prefix of 128:

```
Router# show ipv6 mfib FF03:1::1/128

IP Multicast Forwarding Information Base
Entry Flags:C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop
Forwarding Counts:Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
```

```
Other counts:Total/RPF failed/Other drops
Interface Flags:A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts:FS Pkt Count/PS Pkt Count
(*,FF03:1::1) Flags:C
   Forwarding:0/0/0/0, Other:0/0/0
   Tunnel1 Flags:A NS
   GigabitEthernet5/0.25 Flags:F NS
     Pkts:0/0
   GigabitEthernet5/0.24 Flags:F NS
     Pkts:0/0
.
.
.
   GigabitEthernet5/0.16 Flags:F NS
     Pkts:0/0
```

The following example shows forwarding entries and interfaces in the MFIB, with a group address of FFE0 and a prefix of 15:

```
Router# show ipv6 mfib FFE0::/15

IP Multicast Forwarding Information Base
Entry Flags:C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop
Forwarding Counts:Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts:Total/RPF failed/Other drops
Interface Flags:A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts:FS Pkt Count/PS Pkt Count
(*,FFE0::/15) Flags:D
   Forwarding:0/0/0/0, Other:0/0/0
```

The following example shows output of the **show ipv6 mfib** command used with the **verbose** keyword. It shows forwarding entries and interfaces in the MFIB and additional information such as the MAC encapsulation header and platform-specific information.

```
Router# show ipv6 mfib ff33::1:1 verbose

IP Multicast Forwarding Information Base
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, K - Keepalive
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Platform per slot HW-Forwarding Counts: Pkt Count/Byte Count
Platform flags: HF - Forwarding entry,HB - Bridge entry,HD - NonRPF Drop entry,
                NP - Not platform switchable,RPL - RPF-ltl linkage,
                MCG - Metset change,ERR - S/w Error Flag,RTY - In RetryQ,
                LP - L3 pending,MP - Met pending,AP - ACL pending
Interface Flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: Distributed FS Pkt Count/FS Pkt Count/PS Pkt Count
(10::2,FF33::1:1) Flags: K
   RP Forwarding: 0/0/0/0, Other: 0/0/0
   LC Forwarding: 0/0/0/0, Other: 0/0/0
   HW Forwd:   0/0/0/0, Other: NA/NA/NA
   Slot 6: HW Forwarding: 0/0, Platform Flags:  HF RPL
   Slot 1: HW Forwarding: 0/0, Platform Flags:  HF RPL
   Vlan10 Flags: A
   Vlan30 Flags: F NS
     Pkts: 0/0/0 MAC: 33330001000100D0FFFE180086DD
```

Table 177 describes the fields shown in the display.

Table 177 show ipv6 mfib verbose Field Descriptions

Field	Description
Platform flags	Information about the platform.
Platform per slot HW-Forwarding Counts	Total number of packets per bytes forwarded.

Related Commands

Command	Description
show ipv6 mfib active	Displays the rate at which active sources are sending to multicast groups.
show ipv6 mfib count	Displays summary traffic statistics from the MFIB about the group and source.
show ipv6 mfib interface	Displays information about IPv6 multicast-enabled interfaces and their forwarding status.
show ipv6 mfib status	Displays the general MFIB configuration and operational status.
show ipv6 mfib summary	Displays summary information about the number of IPv6 MFIB entries (including link-local groups) and interfaces.

show ipv6 mfib active

To display the rate at which active sources are sending to multicast groups, use the **show ipv6 mfib active** command in user EXEC or privileged EXEC mode.

show ipv6 mfib [**vrf** *vrf-name*] [**all** | **linkscope**] **active** [*kbps*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
all	(Optional) Displays a summary of traffic statistics from the IPv6 MFIB about multicast sources sending to both linkscope (reserved) and nonlinkscope (nonreserved) groups.
linkscope	(Optional) Displays a summary of traffic statistics from the IPv6 MFIB about multicast sources sending to linkscope (reserved) groups.
kbps	(Optional) Kilobits per second.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	The **link-local** keyword was added.
12.3(4)T	The **link-local** 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.
12.2(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.
15.0(1)M	This command was modified. The **link-local** keyword was changed to **linkscope**.
Cisco IOS Release 15.1(1)S	This command was modified. New counters were added to the output to show (*,G/m) and the total number of unique groups in the database.
Cisco IOS XE Release 3.2S	This command was modified. New counters were added to the output to show (*,G/m) and the total number of unique groups in the database.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

Use the **show ipv6 mfib active** command to display MFIB entries actively used to forward packets. In many cases, it is useful to provide the optional *kbps* argument to limit the set of entries displayed to the ones that are forwarding an amount of traffic larger or equal to the amount set by the *kbps* argument.

Examples

The following example displays statistics on the rate at which active IP multicast sources are sending information. The router is switching traffic from 2001::1:1:200 to FF05::1:

```
Router# show ipv6 mfib active

Active IPv6 Multicast Sources - sending >= 4 kbps
Group: FF05::1
  Source: 2001::1:1:200
    Rate: 20 pps/16 kbps(1sec), 0 kbps(last 128 sec)
```

Table 178 describes the significant fields shown in the display.

Table 178 show ipv6 mfib active Field Descriptions

Field	Description
Group:	Summary information about counters for (*, G) and the range of (S, G) states for one particular group G. The following RP-tree: and Source: output fields contain information about the individual states belonging to this group. **Note** For Source Specific Multicast (PIM-SSM) range groups, the Group: displays are statistical. All SSM range (S, G) states are individual, unrelated SSM channels.
Rate...kbps	Bytes per second divided by packets per second divided by 1000. On an IP multicast fast-switching platform, the number of packets per second is the number of packets during the last second. Other platforms may use a different approach to calculate this number. Refer to the platform documentation for more information.

show ipv6 mfib count

To display summary traffic statistics from the IPv6 Multicast Forwarding Information Base (MFIB) about multicast sources and groups, use the **show ipv6 mfib count** command in user EXEC or privileged EXEC mode.

show ipv6 mfib [**vrf** *vrf-name*] [**all** | **linkscope**] **count**

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
all	(Optional) Displays a summary of traffic statistics from the IPv6 MFIB about multicast sources sending to both linkscope (reserved) and nonlinkscope (nonreserved) groups.
linkscope	(Optional) Displays a summary of traffic statistics from the IPv6 MFIB about multicast sources sending to linkscope (reserved) groups.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	The **link-local** keyword was added.
12.3(4)T	The **link-local** 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.
12.2(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.
15.0(1)M	This command was modified. The **link-local** keyword was changed to **linkscope**.
Cisco IOS Release 15.1(1)S	This command was modified. New counters were added to the output to show (*,G/m) and the total number of unique groups in the database.
Cisco IOS XE Release 3.2S	This command was modified. New counters were added to the output to show (*,G/m) and the total number of unique groups in the database.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

Use the **show ipv6 mfib count** command to display the average packet size and data rate in kilobits per seconds.

Examples

The following example displays a summary of traffic statistics from the IPv6 MFIB about multicast sources sending to both reserved and nonreserved groups:

```
Router# show ipv6 mfib all count
```

show ipv6 mfib global

To display information from the IPv6 Multicast Forwarding Information Base (MFIB) global table, use the **show ipv6 mfib active** command in user EXEC or privileged EXEC mode.

show ipv6 mfib [**vrf** *vrf-name*] [**all** | **linkscope**] **global**

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
all	(Optional) Displays information in the IPv6 MFIB global table for both linkscope (reserved) and nonlinkscope (nonreserved) groups.
linkscope	(Optional) Displays information in the IPv6 MFIB global table for linkscope groups.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	The **link-local** keyword was added.
12.3(4)T	The **link-local** 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.
12.2(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.
15.0(1)M	This command was modified. The **link-local** keyword was changed to **linkscope**.
Cisco IOS Release 15.1(1)S	This command was modified. New counters were added to the output to show (*,G/m) and the total number of unique groups in the database.
Cisco IOS XE Release 3.2S	This command was modified. New counters were added to the output to show (*,G/m) and the total number of unique groups in the database.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

If no optional keywords or arguments are entered, global table information in the IPv6 MFIB associated with nonlinkscope multicast groups are displayed.

Examples

The following example enables you to display IPv6 MFIB global table information:

```
Router# show ipv6 mfib global
```

show ipv6 mfib instance

To display information about an IPv6 Multicast Forwarding Information Base (MFIB) table instance, use the **show ipv6 mfib instance** command in user EXEC or privileged EXEC mode.

show ipv6 mfib [**vrf** *vrf-name*] [**all** | **linkscope**] **instance**

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
all	(Optional) Displays all information about a.
linkscope	(Optional) Displays a summary of traffic statistics from the IPv6 MFIB about multicast sources sending to linkscope (reserved) groups.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	The **link-local** keyword was added.
12.3(4)T	The **link-local** 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.
12.2(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.
15.0(1)M	This command was modified. The **link-local** keyword was changed to **linkscope**.
Cisco IOS Release 15.1(1)S	This command was modified. New counters were added to the output to show (*,G/m) and the total number of unique groups in the database.
Cisco IOS XE Release 3.2S	This command was modified. New counters were added to the output to show (*,G/m) and the total number of unique groups in the database.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Examples

The following example enables you to display IPv6 MFIB instance information:

```
Router# show ipv6 mfib instance
```

show ipv6 mfib interface

To display information about IPv6 multicast-enabled interfaces and their forwarding status, use the **show ipv6 mfib interface** command in user EXEC or privileged EXEC mode.

show ipv6 mfib interface

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)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 introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The **show ipv6 mfib interface** command displays the Multicast Forwarding Information Base (MFIB) interfaces and in what switching mode each MFIB has been configured.

Examples

The following example displays information about IPv6 multicast-enabled interfaces and their forwarding status. The router is configured for fast switching.

```
Router# show ipv6 mfib interface

IPv6 Multicast Forwarding (MFIB) status:
    Configuration Status: enabled
    Operational Status: running

MFIB interface       status    CEF-based output
                             [configured,available]
Ethernet1/1          up      [yes       ,yes      ]
Ethernet1/2          up      [yes       ,?        ]
Tunnel0              up      [yes       ,?        ]
Tunnel1              up      [yes       ,?        ]
```

Table 179 describes the significant fields shown in the display.

Table 179 show ipv6 mfib interface Field Descriptions

Field	Description
MFIB interface	Specifies the MFIB interface.
Status	Specifies the status of the MFIB interface.
CEF-based output	Provides information on the Cisco Express Forwarding-based output of the MFIB interface.

show ipv6 mfib route

To display the forwarding entries and interfaces in the IPv6 Multicast Forwarding Information Base (MFIB) without packet header information and forwarding counters, use the **show ipv6 mfib route** command in user EXEC or privileged EXEC mode.

show ipv6 mfib [**vrf** *vrf-name*] [**all** | **linkscope**] **route**

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
all	(Optional) Displays the forwarding entries and interfaces in the IPv6 MFIB for both linkscope (reserved) and nonlinkscope (nonreserved) groups.
linkscope	(Optional) Displays the forwarding entries and interfaces in the IPv6 MFIB for linkscope (reserved) groups.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	The **link-local** keyword was added.
12.3(4)T	The **link-local** 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.
12.2(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.
15.0(1)M	This command was modified. The **link-local** keyword was changed to **linkscope**.
Cisco IOS Release 15.1(1)S	This command was modified. New counters were added to the output to show (*,G/m) and the total number of unique groups in the database.
Cisco IOS XE Release 3.2S	This command was modified. New counters were added to the output to show (*,G/m) and the total number of unique groups in the database.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Examples

The following example enables you to display IPv6 MFIB instance information:

```
Router# show ipv6 mfib instance
```

show ipv6 mfib status

To display the general Multicast Forwarding Information Base (MFIB) configuration and operational status, use the **show ipv6 mfib status** command in user EXEC or privileged EXEC mode.

show ipv6 mfib status

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.3(4)T	This command was 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.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

Use the **show ipv6 mfib status** to find such information as whether or not MFIB is enabled and running.

Examples

The following example displays MFIB information:

```
Router# show ipv6 mfib status

IPv6 Multicast Forwarding (MFIB) status:
    Configuration Status: enabled
    Operational Status: not running
    Notes: MFIB not running because multicast routing is disabled
```

Table 180 describes the significant fields shown in the displays.

Table 180 show ipv6 mfib status Field Descriptions

Field	Description
Configuration status: enabled	MFIB is enabled on the device.
Operational status: not running	Although MFIB is enabled on the device, it is not running.
Notes:	Information about MFIB configuration and operational status.

show ipv6 mfib summary

To display summary information about the number of IPv6 Multicast Forwarding Information Base (MFIB) entries (including link-local groups) and interfaces, use the **show ipv6 mfib summary** command in user EXEC or privileged EXEC mode.

show ipv6 mfib [**vrf** *vrf-name*] **summary**

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)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 introduced on Cisco ASR 1000 Series Routers.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

The **show ipv6 mfib summary** command shows the IP multicast routing table in abbreviated form. The command displays only the number of MFIB entries, the number of (*, G) and (S, G) entries, and the number of MFIB interfaces specified.

The **show ipv6 mfib summary** command counts all entries, including link-local entries.

Examples

The following example displays summary information about the number of IPv6 MFIB entries and interfaces:

```
Router# show ipv6 mfib summary

IPv6 MFIB summary:
  54     total entries [1 (S,G), 7 (*,G), 46 (*,G/m)]
  17     total MFIB interfaces
```

Table 181 describes the significant fields shown in the display.

Table 181 show ipv6 mfib summary Field Descriptions

Field	Description
54 total entries	Total number of MFIB entries, including the number of (*, G) and (S, G) entries.
17 total MFIB interfaces	Sum of all the MFIB interfaces in all the MFIB entries.

show ipv6 mld groups

To display the multicast groups that are directly connected to the router and that were learned through Multicast Listener Discovery (MLD), use the **show ipv6 mld groups** command in user EXEC or privileged EXEC mode.

show ipv6 mld [**vrf** *vrf-name*] **groups** [**link-local**] [*group-name* | *group-address*] [*interface-type interface-number*] [**detail** | **explicit**]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
link-local	(Optional) Displays the link-local groups.
group-name | *group-address*	(Optional) IPv6 address or name of the multicast group.
interface-type interface-number	(Optional) Interface type and number.
detail	(Optional) Displays detailed information about individual sources.
explicit	(Optional) Displays information about the hosts being explicitly tracked on each interface for each group.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	The **link-local** keyword was added.
12.3(4)T	The **link-local** keyword was added.
12.3(7)T	The **explicit** keyword was added.
12.2(25)S	The **link-local** and **explicit** keywords were added.
12.4(2)T	Information about MLD state limits was added to the command output.
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.
12.2(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 introduced on Cisco ASR 1000 Series Routers.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

If you omit all optional arguments, the **show ipv6 mld groups** command displays by group address and interface type and number all directly connected multicast groups, including link-local groups (where the **link-local** keyword is not available) used.

Examples

The following is sample output from the **show ipv6 mld groups** command. It shows all of the groups joined by Fast Ethernet interface 2/1, including link-local groups used by network protocols.

```
Router# show ipv6 mld groups FastEthernet 2/1

MLD Connected Group Membership
Group Address           Interface           Uptime        Expires
FF02::2                 FastEthernet2/1     3d18h         never
FF02::D                 FastEthernet2/1     3d18h         never
FF02::16                FastEthernet2/1     3d18h         never
FF02::1:FF00:1          FastEthernet2/1     3d18h         00:00:27
FF02::1:FF00:79         FastEthernet2/1     3d18h         never
FF02::1:FF23:83C2       FastEthernet2/1     3d18h         00:00:22
FF02::1:FFAF:2C39       FastEthernet2/1     3d18h         never
FF06:7777::1            FastEthernet2/1     3d18h         00:00:26
```

The following is sample output from the **show ipv6 mld groups** command using the **detail** keyword:

```
Router# show ipv6 mld groups detail

Interface:      Ethernet2/1/1
Group:          FF33::1:1:1
Uptime:         00:00:11
Router mode:    INCLUDE
Host mode:      INCLUDE
Last reporter:  FE80::250:54FF:FE60:3B14
Group source list:
Source Address                          Uptime    Expires   Fwd  Flags
2004:4::6                               00:00:11  00:04:08  Yes  Remote Ac 4
```

The following is sample output from the **show ipv6 mld groups** command using the **explicit** keyword:

```
Router# show ipv6 mld groups explicit

Ethernet1/0, FF05::1
    Up:00:43:11 EXCLUDE(0/1) Exp:00:03:17
    Host Address                            Uptime   Expires
    FE80::A8BB:CCFF:FE00:800                00:43:11 00:03:17
    Mode:EXCLUDE

Ethernet1/0, FF05::6
    Up:00:42:22 INCLUDE(1/0) Exp:not used
    Host Address                            Uptime   Expires
    FE80::A8BB:CCFF:FE00:800                00:42:22 00:03:17
    Mode:INCLUDE
        300::1
        300::2
        300::3

Ethernet1/0 - Interface
ff05::1 - Group address
Up:Uptime for the group
EXCLUDE/INCLUDE - The mode the group is in on the router.
(0/1) (1/0) - (Number of hosts in INCLUDE mode/Number of hosts in EXCLUDE moe)
Exp:Expiry time for the group.
FE80::A8BB:CCFF:FE00:800 - Host ipv6 address.
00:43:11 - Uptime for the host.
00:03:17 - Expiry time for the host
Mode:INCLUDE/EXCLUDE - Mode the Host is operating in.
300::1, 300::2, 300::3 - Sources that the host has joined in the above specified mode.
```

Table 182 describes the significant fields shown in the display.

Table 182 show ipv6 mld groups Field Descriptions

Field	Description
Group Address	Address of the multicast group.
Interface	Interface through which the group is reachable.
Uptime	How long (in hours, minutes, and seconds) this multicast group has been known.
Expires	How long (in hours, minutes, and seconds) until the entry is removed from the MLD groups table. The expiration timer shows "never" if the router itself has joined the group, and the expiration timer shows "not used" when the router mode of the group is INCLUDE. In this situation, the expiration timers on the source entries are used.
Last reporter:	Last host to report being a member of the multicast group.
Flags Ac 4	Flags counted toward the MLD state limits configured.

Related Commands

Command	Description
ipv6 mld query-interval	Configures the frequency at which the Cisco IOS software sends MLD host-query messages.

show ipv6 mld groups summary

To display the number of (*, G) and (S, G) membership reports present in the Multicast Listener Discovery (MLD) cache, use the **show ipv6 mld groups summary** command in user EXEC or privileged EXEC mode.

show ipv6 mld groups summary

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
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.
12.2(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 introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The **show ipv6 mld groups summary** command displays the number of directly connected multicast groups (including link-local groups).

Examples

The following is sample output from the **show ipv6 mld groups summary** command:

```
Router# show ipv6 mld groups summary

MLD Route Summary
  No. of (*,G) routes = 5
  No. of (S,G) routes = 0
```

Table 183 describes the significant fields shown in the display.

Table 183 show ipv6 mld groups summary Field Descriptions

Field	Description
No. of (*,G) routes = 5	Displays the number of groups present in the MLD cache.
No. of (S,G) routes = 0	Displays the number of include and exclude mode sources present in the MLD cache.

show ipv6 mld host-proxy

To display IPv6 MLD host proxy information, use the **show ipv6 mld host-proxy** command in user EXEC or privileged EXEC mode.

show ipv6 mld host-proxy [*interface-type interface-number*] [**group** [*group-address*]]

Syntax Description

interface-type interface-number	(Optional) Interface type and number.
group	(Optional) Displays a list of group entries for which the specified interface is acting as a proxy interface.
group-address	(Optional) Specified group.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **show ipv6 mld host-proxy** command displays MLD proxy information. When this command is used with the *interface-type interface-number* arguments, interface details such as interface state, IPv6 address, MLD state, etc., are displayed. If an interface is not specified, the **show ipv6 mld host-proxy** command displays all active proxy interfaces on the router.

The **show ipv6 mld host-proxy** command when used with the *interface-type interface-number* arguments and the **group** keyword displays information about group entries for which interface is acting as a proxy interface. If the *group-address* argument is specified, it display the group information for specified group.

Examples

The following example displays IPv6 MLD proxy information for the Ethernet 0/0 interface:

```
Router# show ipv6 mld host-proxy Ethernet0/0

Ethernet0/0 is up, line protocol is up
  Internet address is FE80::34/64
MLD is enabled on interface
  MLD querying router is FE80::12, Version: MLDv2
  Current MLD host version is 2
  MLD max query response time is 10 seconds
Number of MLD Query sent on interface : 10
Number of MLD Query received on interface : 20
Number of MLDv1 report sent : 5
Number of MLDv2 report sent : 10
Number of MLDv1 leave sent : 0
Number of MLDv2 leave sent : 1
```

Table 184 describes the significant fields shown in the display.

Table 184 show ipv6 mld host-proxy Field Descriptions

Field	Description
Ethernet0/0 is up, line protocol is up	State of the specified interface.
Internet address is FE80::34/64	IPv6 address of the specified interface.
MLD is enabled on interface	State of MLD on the interface, whether enabled or disabled.
MLD querying router is FE80::12, Version: MLDv2	IPv6 address and MLD version of the querying router.
Current MLD host version is 2	Configured MLD host version.
MLD max query response time is 10 seconds	Maximum allowed response time for the query.
Number of MLD Query sent on interface: 10	Number of MLD queries sent from the interface.
Number of MLD Query received on interface: 20	Number of MLD queries received on the interface.
Number of MLDv1 report sent : 5	Number of MLDv1 membership reports sent.
Number of MLDv2 report sent : 10	Number of MLDv2 membership reports sent.
Number of MLDv1 leave sent : 0	Number of MLDv1 leave reports sent.
Number of MLDv2 leave sent : 1	Number of MLDv2 leave reports sent.

The following example provides information about a group entry for the Ethernet 0/0 proxy interface:

```
Router# show ipv6 mld host-proxy Ethernet0/0 group

Group:               FF5E::12
Uptime:             00:00:07
Group mode:     INCLUDE
Version             MLDv2
Group source list:
  Source Address        Uptime
            5000::2                     00:00:07
            2000::2                     00:01:15

Group:               FF7E::21
Uptime:             00:02:07
Group mode:     EXCLUDE
Version              MLDv2
Group source list: Empty
```

Table 184 describes the significant fields shown in the display.

Table 185 show ipv6 mld host-proxy Field Descriptions

Field	Description
Group: FF5E::12	The IPv6 address of the group.
Uptime: 00:00:07	The length of time the group has been active.
Group mode: INCLUDE	The group mode.
Version MLDv2	The MLD version on the proxy interface.
Group source list:	Information on the group source list.

Related Commands

Command	Description
ipv6 mld host-proxy	Enables the MLD proxy feature.
ipv6 mld host-proxy interface	Enables the MLD proxy feature on a specified interface on an RP.

show ipv6 mld interface

To display multicast-related information about an interface, use the **show ipv6 mld interface** command in user EXEC or privileged EXEC mode.

show ipv6 mld [**vrf** *vrf-name*] **interface** [*type number*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
type number	(Optional) Interface type and number.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.4(2)T	Information about MLD state limits was added to the command output.
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.
12.2(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 introduced on Cisco ASR 1000 Series Routers.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

If you omit the optional *type* and *number* arguments, the **show ipv6 mld interface** command displays information about all interfaces.

Examples

The following is sample output from the **show ipv6 mld interface** command for Ethernet interface 2/1/1:

```
Router# show ipv6 mld interface Ethernet 2/1/1

Global State Limit : 2 active out of 2 max
Loopback0 is administratively down, line protocol is down
  Internet address is ::/0
.
.
.
Ethernet2/1/1 is up, line protocol is up
  Internet address is FE80::260:3EFF:FE86:5649/10
  MLD is enabled on interface
  Current MLD version is 2
  MLD query interval is 125 seconds
  MLD querier timeout is 255 seconds
```

```
MLD max query response time is 10 seconds
Last member query response interval is 1 seconds
Interface State Limit : 2 active out of 3 max
State Limit permit access list:
MLD activity: 83 joins, 63 leaves
MLD querying router is FE80::260:3EFF:FE86:5649 (this system)
```

Table 186 describes the significant fields shown in the display.

Table 186 show ipv6 mld interface Field Descriptions

Field	Description
Global State Limit: 2 active out of 2 max	Two globally configured MLD states are active.
Ethernet2/1/1 is up, line protocol is up	Interface type, number, and status.
Internet address is...	Internet address of the interface and subnet mask being applied to the interface.
MLD is enabled in interface	Indicates whether Multicast Listener Discovery (MLD) has been enabled on the interface with the **ipv6 multicast-routing** command.
Current MLD version is 2	The current MLD version.
MLD query interval is 125 seconds	Interval (in seconds) at which the Cisco IOS software sends MLD query messages, as specified with the **ipv6 mld query-interval** command.
MLD querier timeout is 255 seconds	The length of time (in seconds) before the router takes over as the querier for the interface, as specified with the **ipv6 mld query-timeout** command.
MLD max query response time is 10 seconds	The length of time (in seconds) that hosts have to answer an MLD Query message before the router deletes their group, as specified with the **ipv6 mld query-max-response-time** command.
Last member query response interval is 1 seconds	Used to calculate the maximum response code inserted in group and source-specific query. Also used to tune the “leave latency” of the link. A lower value results in reduced time to detect the last member leaving the group.
Interface State Limit : 2 active out of 3 max	Two out of three configured interface states are active.
State Limit permit access list: change	Activity for the state permit access list.
MLD activity: 83 joins, 63 leaves	Number of groups joins and leaves that have been received.
MLD querying router is FE80::260:3EFF:FE86:5649 (this system)	IPv6 address of the querying router.

Related Commands

Command	Description
ipv6 mld join-group	Configures MLD reporting for a specified group and source.
ipv6 mld query-interval	Configures the frequency at which the Cisco IOS software sends MLD host-query messages.

show ipv6 mld snooping

To display Multicast Listener Discovery version 2 (MLDv2) snooping information, use the **show ipv6 mld snooping** command in privileged EXEC mode.

show ipv6 mld [**vrf** *vrf-name*] **snooping** {**explicit-tracking vlan** *vlan* | **mrouter** [**vlan** *vlan*] | **report-suppression vlan** *vlan* | **statistics vlan** *vlan*}

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
explicit-tracking vlan *vlan*	Displays the status of explicit host tracking.
mrouter	Displays the multicast router interfaces on an optional VLAN.
vlan *vlan*	(Optional) Specifies the VLAN number on the multicast router interfaces.
report-suppression vlan *vlan*	Displays the status of the report suppression.
statistics vlan *vlan*	Displays MLD snooping information on a VLAN.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXE	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.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

You can enter the **show ipv6 mld snooping mrouter** command without arguments to display all the multicast router interfaces.

Examples

This example shows how to display explicit tracking information on VLAN 25:

```
Router# show ipv6 mld snooping explicit-tracking vlan 25

Source/Group                    Interface    Reporter        Filter_mode
--------------------------------------------------------------------------
10.1.1.1/226.2.2.2              Vl25:1/2     10.27.2.3       INCLUDE
10.2.2.2/226.2.2.2              Vl25:1/2     10.27.2.3       INCLUDE
```

This example shows how to display the multicast router interfaces in VLAN 1:

```
Router# show ipv6 mld snooping mrouter vlan 1

vlan            ports
-----+---------------------------------------
```

```
  1          Gi1/1,Gi2/1,Fa3/48,Router
```

This example shows the MLD snooping statistics information for VLAN 25:

```
Router# show ipv6 mld snooping statistics interface vlan 25

Snooping staticstics for Vlan25
#channels:2
#hosts   :1

Source/Group            Interface       Reporter      Uptime        Last-Join   Last-Leave
10.1.1.1/226.2.2.2      Gi1/2:Vl25      10.27.2.3     00:01:47      00:00:50      -
10.2.2.2/226.2.2.2      Gi1/2:Vl25      10.27.2.3     00:01:47      00:00:50      -
```

Related Commands

Command	Description
ipv6 mld snooping	Enables MLDv2 snooping globally.
ipv6 mld snooping explicit-tracking	Enables explicit host tracking.
ipv6 mld snooping querier	Enables the MLDv2 snooping querier.
ipv6 mld snooping report-suppression	Enables report suppression on a VLAN.

show ipv6 mld ssm-map

To display Source Specific Multicast (SSM) mapping information, use the **show ipv6 mld ssm-map static** command in user EXEC or privileged EXEC mode.

show ipv6 mld [**vrf** *vrf-name*] **ssm-map** [*source-address*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
source-address	(Optional) Source address associated with an MLD membership for a group identified by the access list.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(18)SXE	This command was introduced.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
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.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

If the optional *source-address* argument is not used, all SSM mapping information is displayed.

Examples

The following example shows all SSM mappings for the router:

```
Router# show ipv6 mld ssm-map

SSM Mapping  : Enabled
DNS Lookup   : Enabled
```

The following examples show SSM mapping for the source address 2001:0DB8::1:

```
Router# show ipv6 mld ssm-map 2001:0DB8::1

 Group address  : 2001:0DB8::1
 Group mode ssm : TRUE
 Database       : STATIC
 Source list    : 2001:0DB8::2
                  2001:0DB8::3

Router# show ipv6 mld ssm-map 2001:0DB8::2

 Group address  : 2001:0DB8::2
 Group mode ssm : TRUE
 Database       : DNS
 Source list    : 2001:0DB8::3
```

```
2001:0DB8::1
```

Table 187 describes the significant fields shown in the displays.

Table 187 show ipv6 mld ssm-map Field Descriptions

Field	Description
SSM Mapping	The SSM mapping feature is enabled.
DNS Lookup	The DNS lookup feature is automatically enabled when the SSM mapping feature is enabled.
Group address	Group address identified by a specific access list.
Group mode ssm : TRUE	The identified group is functioning in SSM mode.
Database : STATIC	The router is configured to determine source addresses by checking static SSM mapping configurations.
Database : DNS	The router is configured to determine source addresses using DNS-based SSM mapping.
Source list	Source address associated with a group identified by the access list.

Related Commands

Command	Description
debug ipv6 mld ssm-map	Displays debug messages for SSM mapping.
ipv6 mld ssm-map enable	Enables the SSM mapping feature for groups in the configured SSM range
ipv6 mld ssm-map query dns	Enables DNS-based SSM mapping.
ipv6 mld ssm-map static	Configures static SSM mappings.

show ipv6 mld traffic

To display the Multicast Listener Discovery (MLD) traffic counters, use the **show ipv6 mld traffic** command in user EXEC or privileged EXEC mode.

show ipv6 mld [**vrf** *vrf-name*] **traffic**

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.3(4)T	This command was 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.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

Use the **show ipv6 mld traffic** command to check if the expected number of MLD protocol messages have been received and sent.

Examples

The following example displays the MLD protocol messages received and sent.

```
Router# show ipv6 mld traffic

MLD Traffic Counters
Elapsed time since counters cleared:00:00:21

                                 Received     Sent
Valid MLD Packets                  3           1
Queries                            1           0
Reports                            2           1
Leaves                             0           0
Mtrace packets                     0           0

Errors:
Malformed Packets                              0
Bad Checksums                                  0
Martian source                                 0
Packets Received on MLD-disabled Interface     0
```

Table 188 describes the significant fields shown in the display.

Table 188 show ipv6 mld traffic Field Descriptions

Field	Description
Elapsed time since counters cleared	Indicates the amount of time (in hours, minutes, and seconds) since the counters cleared.
Valid MLD packets	Number of valid MLD packets received and sent.
Queries	Number of valid queries received and sent.
Reports	Number of valid reports received and sent.
Leaves	Number of valid leaves received and sent.
Mtrace packets	Number of multicast trace packets received and sent.
Errors	Types of errors and the number of errors that have occurred.

show ipv6 mobile binding

To display information about the binding cache, use the **show ipv6 mobile binding** command in user EXEC or privileged EXEC mode.

show ipv6 mobile binding [**care-of-address** *address* | **home-address** *address* | *interface-type interface-number*]

Syntax Description

care-of-address	(Optional) Provides information about the mobile node's current location.
address	(Optional) Current address of the mobile node.
home-address	(Optional) IPv6 address is assigned to the mobile node within its home subnet prefix on its home link.
interface-type interface-number	(Optional) Interface type and number.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(11)T	Command output was updated to display the tunnel interface and the tunnel end point details.

Usage Guidelines

The **show ipv6 mobile binding** command displays details of all bindings that match all search criteria. If no optional keywords or arguments are specified, all bindings are displayed.

Examples

The following example displays information about the binding cache:

```
Router# show ipv6 mobile binding

Mobile IPv6 Binding Cache Entries:

  2001:1::8
    via care-of address 2001:2::1
    home-agent 2001:1::2
    state ACTIVE, sequence 1, flags AHrlK
    lifetime:remaining 1023 (secs), granted 1024 (secs), requested 1024 (secs)
    interface Ethernet1/3
    0 tunneled, 0 reversed tunneled
Selection matched 1 bindings
```

The following example displays information about the tunnel interface and the tunnel end point details:

```
Router# show ipv6 mobile bindings
```

```
Tunnel Interface: tunnel0
Tunnel Source 2001:0DB1:1:1
Tunnel Destination: 2001:0DB1:2:1
Input: 20 packets, 1200 bytes, 0 drops
Output: 20 packets, 1200 bytes, 0 drops
```

Table 180 describes the significant fields shown in the displays.

Table 189 show ipv6 mobile binding Field Descriptions

Field	Description
2001:1::8	Home IPv6 address of the mobile node.
via care-of address 2001:2::1	Care-of address of the mobile node.
home-agent 2001:1::2	Home-agent address
state ACTIVE, sequence 1, flags AHrlK	• State: State of the mobile binding. • Sequence number. • Flags: Services requested by mobile node. The mobile node requests these services by setting bits in the registration request. Uppercase characters denote bit set.
lifetime:remaining 1023 (secs), granted 1024 (secs), requested 1024 (secs)	• Remaining: The time remaining until the registration is expired. It has the same initial value as lifetime granted, and is counted down by the home agent. • Granted: The lifetime granted to the mobile node for this registration. Number of seconds in parentheses. • Requested: The lifetime requested by the mobile node for this registration. Number of seconds in parentheses.
interface Ethernet1/3	The interface being used.
0 tunneled, 0 reversed tunneled	Number of bindings tunneled and reverse tunneled.
Selection matched 1 bindings	Total number of mobility bindings that were matched.
Tunnel Interface	The tunnel interface being used.
Tunnel Source	Tunnel source IPv6 address.
Tunnel Destionation	Tunnel destination IPv6 address.
Input	Number of packets in.
Output	Number of packets out.

Related Commands

binding	Configures binding options for the Mobile IPv6 home agent feature in home-agent configuration mode.
ipv6 mobile home-agent (interface configuration)	Initializes and starts the Mobile IPv6 home agent on a specific interface.

show ipv6 mobile globals

To display global Mobile IPv6 parameters, use the **show ipv6 mobile globals** command in user EXEC or privileged EXEC mode.

show ipv6 mobile globals

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(11)T	Command output was updated to show the Mobile IPv6 tunnel information on the home agent.

Usage Guidelines

The **show ipv6 mobile globals** command displays the values of all global configuration parameters associated with Mobile IPv6 and lists the interfaces on which home agent functionality is operating.

Examples

In the following example, the **show ipv6 mobile globals** command displays the binding parameters:

```
Router# show ipv6 mobile globals

Mobile IPv6 Global Settings:

  1 Home Agent service on following interfaces:
    Ethernet1/2
  Bindings:
    Maximum number is unlimited.
    1 bindings are in use
    1 bindings peak
    Binding lifetime permitted is 262140 seconds
    Recommended refresh time is 300 seconds
```

In the following example, the **show ipv6 mobile globals** command displays the Mobile IPv6 tunnel information parameters on the home agent:

```
Router# show ipv6 mobile globals

Tunnel Encapsulation Mode: IPv6/IPv6
ICMP Unreachable for tunnel interfaces <enabled/disabled>
Tunnel Path MTU Discovery: <enabled/disabled>
```

Table 180 describes the significant fields shown in the displays.

Table 190 show ipv6 mobile globals Field Descriptions

Field	Description
1 Home Agent service on following interfaces: Ethernet1/2	Interface on which the home agent service is enabled.
Bindings:	Information on bindings.
Maximum number is unlimited.	The amount of bindings allowed on the home agent.
1 bindings are in use.	How many bindings are being used.
1 bindings peak	The maximum number of bindings that have been used in this session.
Binding lifetime permitted is 262140 seconds	The configured binding lifetime.
Recommended refresh time is 300 seconds	The configured refresh time.
Tunnel Encapsulation Mode:	Tunnel encapsulation type.
ICMP Unreachable for tunnel interfaces	Enabled or disabled.
Tunnel Path MTU Discovery:	Enabled or disabled.

Related Commands

Command	Description
address (IPv6 mobile router)	Specifies the home address of the IPv6 mobile node.
binding	Configures binding options for the Mobile IPv6 home agent feature in home agent configuration mode.
ipv6 mobile home-agent (global configuration)	Enters home agent configuration mode.
host group	Creates a host configuration in Mobile IPv6.

show ipv6 mobile home-agents

To display local and discovered neighboring home agents, use the **show ipv6 mobile home-agents** command in user EXEC or privileged EXEC mode.

show ipv6 mobile home-agents [*interface-type interface-number* [*prefix*]]

Syntax Description

interface-type interface-number	(Optional) Interface type and number.
prefix	(Optional) IPv6 address prefix of the care-of address or the home address of neighboring agents.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

The **show ipv6 mobile home-agents** command displays information about local and discovered neighboring home agents. You can choose to display information on a specified interface using the optional *interface-type* and *interface-number* arguments, and you can further choose to display only those addresses that match the optional *prefix* argument.

If no argument or keyword is entered, the home agent list for each interface on which the router is acting as a home agent is displayed. Each list is displayed in decreasing order of preference.

Examples

In the following example, the fact that no neighboring mobile home agents were found is displayed:

```
Router# show ipv6 mobile home-agents

Home Agent information for Ethernet1/3
  Configured:
    FE80::20B:BFFF:FE33:501F
    preference 0 lifetime 1800
      global address 2001:0DB8:1::2/64
  Discovered Home Agents:
    FE80::4, last update 0 min
    preference 0 lifetime 1800
      global address 2001:0DB8:1::4/64
```

Table 180 describes the significant fields shown in the display.

Table 191 show ipv6 mobile home-agents Field Descriptions

Field	Description
Home Agent information for Ethernet1/3	The interface on which the home agent is configured.
Configured: FE80::20B:BFFF:FE33:501F	The IPv6 address on which the home agent is configured.
preference 0 lifetime 1800	The configured home agent preference and lifetime.
global address 2001:0DB8:1::2/64	The configured global address.
Discovered Home Agents: FE80::4, last update 0 min preference 0 lifetime 1800 global address 2001:0DB8:1::4/64	The address and configuration information about discovered home agents.

Related Commands

Command	Description
binding	Configures binding options for the Mobile IPv6 home agent feature in home agent configuration mode.

show ipv6 mobile host groups

To display information about IPv6 mobile host groups, use the **show ipv6 mobile host groups** command in user EXEC or privileged EXEC mode.

show ipv6 mobile host groups [*profile-name*]

Syntax Description

profile-name	(Optional) Host group profile name.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

The **show ipv6 mobile host groups** command lists the configuration of all configured host groups. To display information about a specific host group, use the optional *profile-name* keyword.

Examples

In the following example, information about a host group named localhost is displayed:

```
Router# show ipv6 mobile host groups

Mobile IPv6 Host Configuration
Mobile Host List:

Host Group Name: localhost
    NAI: sai@cisco.com
    Address: CAB:C0:CA5A:CA5A::CA5A

    Security Association Entry:
      SPI: (Hex: 501) (Decimal Int: 1281)
      Key Format: Hex    Key: baba
      Algorithm: HMAC_SHA1
      Replay Protection: On    Replay Window: 6 secs
```

Table 180 describes the significant fields shown in the display.

Table 192 show ipv6 mobile host groups Field Descriptions

Field	Description
Host Group Name: localhost	Configuration information about the host group named localhost to follow.
NAI: sai@cisco.com	Network access identifier (NAI) for localhost host group.
Address: 2001:0DB8:CA5A:CA5A::CA5A	IPv6 address for localhost host group.

Table 192 show ipv6 mobile host groups Field Descriptions (continued)

Field	Description
Security Association Entry:	Security association for the host group named localhost to follow.
SPI: (Hex: 501) (Decimal Int: 1281)	SPI for localhost.
Key Format: Hex Key: baba	Key format and name for localhost.
Algorithm: HMAC_SHA1	Authentication algorithm.
Replay Protection: On Replay Window: 6 secs	Replay protection is activated, and the number of seconds that the router uses for replay protection is 6.

Related Commands

Command	Description
address (Mobile IPv6)	Specifies the home address of the IPv6 mobile node.
authentication (Mobile IPv6)	Specifies the authentication properties for the IPv6 mobile node by creating either a unidirectional or bidirectional SPI.
host group	Creates a host group configuration in IPv6 Mobile.
nai	Specifies the NAI for the IPv6 mobile node.
show ipv6 mobile globals	Displays global Mobile IPv6 parameters.

show ipv6 mobile router

To display configuration information and monitoring statistics about the IPv6 mobile router, use the **show ipv6 mobile router** command in user EXEC or privileged EXEC mode.

show ipv6 mobile router [**running-config** | **status**]

Syntax Description

running-config	(Optional) Displays IPv6 mobile router running configuration information.
status	(Optional) Displays IPv6 mobile router status information.

Command Modes

User EXEC
Privileged EXEC

Command History

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

Usage Guidelines

The **show ipv6 mobile router** display includes the mobile router configuration information such as the home address and network mask, home agent, and registration settings, and operational information such as status, tunnel interface, active foreign agent, and care-of address.

Examples

The following is sample output from the **show ipv6 mobile router** command:

```
Router# show ipv6 mobile router

Mobile Reverse Tunnel established
---------------------------------
using Nemo Basic mode
Home Agent: 2001:DB8:2000::2001
CareOf Address: 2001:DB8::A8BB:CCFF:FE01:F611
Attachment Router: FE80::A8BB:CCFF:FE01:F511
Attachment Interface: Ethernet1/1
Home Network: 2001:DB8:2000:0:FDFF:FFFF:FFFF:FFFE/64
Home Address: 2001:DB8:2000::1111
```

Table 193 describes the significant fields shown in the display.

Table 193 show ipv6 mobile router Field Descriptions

Field	Description
Mobile Reverse Tunnel established	If reverse tunnel is enabled or disabled, this information is displayed or absent, respectively.
using Nemo Basic mode	Type of mode being used by the mobile router.
Home Agent:	Home agent with which the mobile router registers. The mobile router registers only to the home agent with the highest priority when multiple addresses are configured.

Table 193 show ipv6 mobile router Field Descriptions (continued)

Field	Description
CareOf Address:	Care-of address used by the registered mobile router.
Attachment Router:	Attachment point in the foreign network.
Attachment Interface:	Attachment interface used in the foreign network.
Home Network:	IPv6 address of the mobile router home network.
Home Address:	IPv6 address of the mobile router.

show ipv6 mobile traffic

To display information about binding updates received and binding acknowledgments sent, use the **show ipv6 mobile traffic** command in user EXEC or privileged EXEC mode.

show ipv6 mobile traffic

Syntax Description

The command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

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.

Usage Guidelines

The **show ipv6 mobile traffic** command displays counters and other information associated with Mobile IPv6. The following counters are maintained globally across all interfaces:

- Dynamic home agent discovery requests received
- Binding updates received
- Home agent registrations received
- Successful home agent registrations
- Home agent deregistrations (lifetime of zero or care-of address equals home address)
- Home agent registrations rejected, defined in the status as sent in the binding acknowledgment with a separate counter for every reason code defined in Table 194, and generated by the implementation
- Time of last registration acceptance
- Time of last registration denial
- Status code for last registration denial
- Binding updates discarded through rate limiting
- Binding acknowledgments discarded through rate limiting
- Binding cache high-water mark, maintained and displayed for registrations

Table 194 shows possible binding status values and reasons for use of these values.

Table 194 show ipv6 mobile traffic Field Descriptions

Reason Code	Binding Status Value
0	Binding update accepted
128	Reason unspecified
129	Administratively prohibited

Table 194 show ipv6 mobile traffic Field Descriptions

Reason Code	Binding Status Value
130	Insufficient resources
131	Home registration not supported
132	Not home subnet
133	Not home agent for this mobile node
134	Duplicate address detection (DAD) failed
135	Sequence number out of window

Examples

In the following example, information about IPv6 Mobile traffic is displayed:

```
Router# show ipv6 mobile traffic

    MIPv6 statistics:
      Rcvd: 6477 total
          0 truncated, 0 format errors
          0 checksum errors
        Binding Updates received:6477
          0 no HA option, 0 BU's length
          0 options' length, 0 invalid CoA
      Sent: 6477 generated
        Binding Acknowledgements sent:6477
          6477 accepted (0 prefix discovery required)
          0 reason unspecified, 0 admin prohibited
          0 insufficient resources, 0 home reg not supported
          0 not home subnet, 0 not home agent for node
          0 DAD failed, 0 sequence number
        Binding Errors sent:0
          0 no binding, 0 unknown MH

  Home Agent Traffic:
    6477 registrations, 0 deregistrations
    00:00:23 since last accepted HA registration
    unknown time since last failed HA registration
    unknown last failed registration code
    Traffic forwarded:
      0 tunneled, 0 reversed tunneled
    Dynamic Home Agent Address Discovery:
      1 requests received, 1 replies sent
    Mobile Prefix Discovery:
      0 solicitations received, 0 advertisements sent
```

Table 195 describes the significant fields shown in the display.

Table 195 show ipv6 mobile traffic Field Descriptions

Field	Description
MIPv6 statistics:	Information about binding updates received by the mobility agent.
Sent:	Information about binding acknowledgments sent by the mobility agent.
Binding Errors sent:	Information about binding errors sent by the mobility agent.

Table 195 show ipv6 mobile traffic Field Descriptions (continued)

Field	Description
Home Agent Traffic: 6477 registrations, 0 deregistrations	Number of registrations and deregistrations accepted by the home agent.
00:00:23 since last accepted HA registration	Length of time since the last registration was accepted by the home agent.
unknown time since last failed HA registration	Length of time since the last failed registration by the home agent.
unknown last failed registration code	Reason why the registration failed, if it did fail.
Dynamic Home Agent Address Discovery:	Number of dynamic home agent discovery requests received and replies sent.
Mobile Prefix Discovery:	Number of mobile prefix discovery solicitations received and advertisements sent by the home agent.

Related Commands

Command	Description
binding	Configures binding options for the Mobile IPv6 home agent feature in home agent configuration mode.

show ipv6 mobile tunnels

To list the Mobile IPv6 tunnels on the home agent, use the **show ipv6 mobile tunnels** command in user EXEC or privileged EXEC mode.

show ipv6 mobile tunnels [**summary** | **tunnel** *if-number*]

Syntax Description

tunnel *if-number*	(Optional) Tunnel interface.
summary	(Optional) Summary of tunnels on the home agent.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

The **show ipv6 mobile tunnels** command displays active tunnels on the Mobile IPv6 home agent. Use the **summary** keyword to view a summary of all tunnels on the home agent, or the **tunnel** *if-number* keyword and argument to view information on a specific tunnel.

Examples

The following example displays information about the Mobile IPv6 tunnels on the home agent:

```
Router# show ipv6 mobile tunnels

Tunnel1:
 Source: 2001:0DB1:1:1
 Destination: 2001:0DB1:2:1
 Encapsulation Mode: IPv6/IPv6
 Egress Interface: Ethernet 1/0
 Switching Mode: Process
 Keep-Alive: Not Supported
 Path MTU Discovery: Enabled
 Input: 20 packets, 1200 bytes, 0 drops
 Output: 20 packets, 1200 bytes, 0 drops
 NEMO Options: Not Supported
```

Table 180 describes the significant fields shown in the display.

Table 196 show ipv6 mobile tunnels Field Descriptions

Field	Description
Source:	Source IPv6 tunnel address.
Destination:	Destination IPv6 tunnel address.
Encapsulation Mode:	Tunnel encapsulation type.
Egress interface:	Interface used for egress (outgoing packets).

Table 196 show ipv6 mobile tunnels Field Descriptions (continued)

Field	Description
Switching mode:	Type of switching mode used.
Keep-alive:	Supported or not supported.
Path MTU Discovery:	Enabled or disabled.
Input:	Number of packets in.
Output:	Number of packets out.
NEMO Options:	Supported or not supported.

Related Commands

Command	Description
show ipv6 mobile home-agent	Displays local and discovered neighboring home agents.

show ipv6 mrib client

To display information about the clients of the Multicast Routing Information Base (MRIB), use the **show ipv6 mrib client** command in user EXEC or privileged EXEC mode.

show ipv6 mrib [**vrf** *vrf-name*] **client** [**filter**] [**name** {*client-name* | *client-name*:*client-id*}]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
filter	(Optional) Displays information about MRIB flags that each client owns and that each client is interested in.
name	(Optional) The name of a multicast routing protocol that acts as a client of MRIB, such as Multicast Listener Discovery (MLD) and Protocol Independent Multicast (PIM).
client-name:*client-id*	The name and ID of a multicast routing protocol that acts as a client of MRIB, such as MLD and PIM. The colon is required.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
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 introduced on Cisco ASR 1000 Series Routers.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

Use the **filter** keyword to display information about the MRIB flags each client owns and the flags in which each client is interested.

Examples

The following is sample output from the **show ipv6 mrib client** command:

```
Router# show ipv6 mrib client

IP MRIB client-connections
igmp:145        (connection id 0)
pim:146 (connection id 1)
mfib ipv6:3     (connection id 2)
slot 3  mfib ipv6 rp agent:16   (connection id 3)
slot 1  mfib ipv6 rp agent:16   (connection id 4)
slot 0  mfib ipv6 rp agent:16   (connection id 5)
```

```
slot 4  mfib ipv6 rp agent:16   (connection id 6)
slot 2  mfib ipv6 rp agent:16   (connection id 7)
```

Table 197 describes the significant fields shown in the display.

Table 197 show ipv6 mrib client Field Descriptions

Field	Description
igmp:145 (connection id 0) pim:146 (connection id 1) mfib ipv6:3 (connection id 2) mfib ipv6 rp agent:16 (connection id 3)	Client ID (client name:process ID)

show ipv6 mrib route

To display Multicast Routing Information Base (MRIB) route information, use the **show ipv6 mrib route** command in user EXEC or privileged EXEC mode.

show ipv6 mrib [**vrf** *vrf-name*] **route** [**link-local** | **summary** | [*sourceaddress-or-name* | *] [*groupname-or-address* [*prefix-length*]]]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
link-local	(Optional) Displays the link-local groups.
summary	(Optional) Displays the number of MRIB entries (including link-local groups) and interfaces present in the MRIB table.
sourceaddress-or-name	(Optional) IPv6 address or name of the source.
*	(Optional) Displays all MRIB route information.
groupname-or-address	(Optional) IPv6 address or name of the multicast group.
prefix-length	(Optional) IPv6 prefix length.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	The **link-local** keyword was added.
12.3(4)T	The **link-local** keyword was added.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
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 introduced on Cisco ASR 1000 Series Routers.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

All entries are created by various clients of the MRIB, such as Multicast Listener Discovery (MLD), Protocol Independent Multicast (PIM), and Multicast Forwarding Information Base (MFIB). The flags on each entry or interface serve as a communication mechanism between various clients of the MRIB. The entries reveal how PIM sends register messages for new sources and the action taken.

The **summary** keyword shows the count of all entries, including link-local entries.

The interface flags are described in Table 198.

Table 198 Description of Interface Flags

Flag	Description
F	Forward—Data is forwarded out of this interface
A	Accept—Data received on this interface is accepted for forwarding
IC	Internal copy
NS	Negate signal
DP	Do not preserve
SP	Signal present
II	Internal interest
ID	Internal uninterest
LI	Local interest
LD	Local uninterest
C	Perform directly connected check

Special entries in the MRIB indicate exceptions from the normal behavior. For example, no signaling or notification is necessary for arriving data packets that match any of the special group ranges. The special group ranges are as follows:

- Undefined scope (FFX0::/16)
- Node local groups (FFX1::/16)
- Link-local groups (FFX2::/16)
- Source Specific Multicast (SSM) groups (FF3X::/32).

For all the remaining (usually sparse-mode) IPv6 multicast groups, a directly connected check is performed and the PIM notified if a directly connected source arrives. This procedure is how PIM sends register messages for new sources.

Examples

The following is sample output from the **show ipv6 mrib route** command using the **summary** keyword:

```
Router# show ipv6 mrib route summary

MRIB Route-DB Summary
  No. of (*,G) routes = 52
  No. of (S,G) routes = 0
  No. of Route x Interfaces (RxI) = 10
```

Table 199 describes the significant fields shown in the display.

Table 199 show ipv6 mrib route Field Descriptions

Field	Description
No. of (*, G) routes	Number of shared tree routes in the MRIB.
No. of (S, G) routes	Number of source tree routes in the MRIB.
No. of Route x Interfaces (RxI)	Sum of all the interfaces on each MRIB route entry.

show ipv6 mroute

To display the information in the PIM topology table in a format similar to the **show ip mroute** command, use the **show ipv6 mroute** command in user EXEC or privileged EXEC mode.

show ipv6 mroute [**vrf** *vrf-name*] [**link-local** | [*group-name* | *group-address* [*source-address* | *source-name*]] [**summary**] [**count**]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
link-local	(Optional) Displays the link-local groups.
group-name | *group-address*	(Optional) IPv6 address or name of the multicast group.
source-address | *source-name*	(Optional) IPv6 address or name of the source.
summary	(Optional) Displays a one-line, abbreviated summary of each entry in the IPv6 multicast routing table.
count	(Optional) Displays statistics from the Multicast Forwarding Information Base (MFIB) about the group and source, including number of packets, packets per second, average packet size, and bytes per second.

Command Default

The **show ipv6 mroute** command displays all groups and sources.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	The **link-local** keyword was added.
12.3(4)T	The **link-local** keyword was added.
12.2(25)S	The **link-local** 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.
12.2(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.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

The IPv6 multicast implementation does not have a separate mroute table. For this reason, the **show ipv6 mroute** command enables you to display the information in the PIM topology table in a format similar to the **show ip mroute** command.

If you omit all optional arguments and keywords, the **show ipv6 mroute** command displays all the entries in the PIM topology table (except link-local groups where the **link-local** keyword is available).

The Cisco IOS software populates the PIM topology table by creating (S,G) and (*,G) entries based on PIM protocol messages, MLD reports, and traffic. The asterisk (*) refers to all source addresses, the "S" refers to a single source address, and the "G" is the destination multicast group address. In creating (S, G) entries, the software uses the best path to that destination group found in the unicast routing table (that is, through Reverse Path Forwarding [RPF]).

Use the **show ipv6 mroute** command to display the forwarding status of each IPv6 multicast route.

Examples

The following is sample output from the **show ipv6 mroute** command:

```
Router# show ipv6 mroute ff07::1

Multicast Routing Table
Flags:D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers:Uptime/Expires
Interface state:Interface, State

(*, FF07::1), 00:04:45/00:02:47, RP 2001:0DB8:6::6, flags:S
  Incoming interface:Tunnel5
  RPF nbr:6:6:6::6
  Outgoing interface list:
    POS4/0, Forward, 00:04:45/00:02:47

(2001:0DB8:999::99, FF07::1), 00:02:06/00:01:23, flags:SFT
  Incoming interface:POS1/0
  RPF nbr:2001:0DB8:999::99
  Outgoing interface list:
    POS4/0, Forward, 00:02:06/00:03:27
```

The following is sample output from the **show ipv6 mroute** command with the **summary** keyword:

```
Router# show ipv6 mroute ff07::1 summary

Multicast Routing Table
Flags:D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers:Uptime/Expires
Interface state:Interface, State

(*, FF07::1), 00:04:55/00:02:36, RP 2001:0DB8:6::6, OIF count:1, flags:S

(2001:0DB8:999::99, FF07::1), 00:02:17/00:01:12, OIF count:1, flags:SFT
```

The following is sample output from the **show ipv6 mroute** command with the **count** keyword:

```
Router# show ipv6 mroute ff07::1 count

IP Multicast Statistics
71 routes, 24 groups, 0.04 average sources per group
Forwarding Counts:Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
Other counts:Total/RPF failed/Other drops(OIF-null, rate-limit etc)
Group:FF07::1
  RP-tree:
   RP Forwarding:0/0/0/0, Other:0/0/0
```

```
 LC Forwarding:0/0/0/0, Other:0/0/0
Source:2001:0DB8:999::99,
 RP Forwarding:0/0/0/0, Other:0/0/0
 LC Forwarding:0/0/0/0, Other:0/0/0
 HW Forwd:  20000/0/92/0, Other:0/0/0
Tot. shown:Source count:1, pkt count:20000
```

Table 200 describes the significant fields shown in the display.

Table 200 show ipv6 mroute Field Descriptions

Field	Description
Flags:	Provides information about the entry. • S—sparse. Entry is operating in sparse mode. • s—SSM group. Indicates that a multicast group is within the SSM range of IP addresses. This flag is reset if the SSM range changes. • C—connected. A member of the multicast group is present on the directly connected interface. • L—local. The router itself is a member of the multicast group. • I—received source specific host report. Indicates that an (S, G) entry was created by an (S, G) report. This flag is set only on the designated router (DR). • P—pruned. Route has been pruned. The Cisco IOS software keeps this information so that a downstream member can join the source. • R—RP-bit set. Indicates that the (S, G) entry is pointing toward the RP. This is typically prune state along the shared tree for a particular source. • F—register flag. Indicates that the software is registering for a multicast source. • T—SPT-bit set. Indicates that packets have been received on the shortest path source tree.
	• J—join SPT. For (*, G) entries, indicates that the rate of traffic flowing down the shared tree is exceeding the SPT-Threshold value set for the group. (The default SPT-Threshold setting is 0 kbps.) When the J - Join shortest path tree (SPT) flag is set, the next (S, G) packet received down the shared tree triggers an (S, G) join in the direction of the source, thereby causing the router to join the source tree. The default SPT-Threshold value of 0 kbps is used for the group, and the J - Join SPT flag is always set on (*, G) entries and is never cleared. The router immediately switches to the shortest path source tree when traffic from a new source is received.
Timers: Uptime/Expires	“Uptime” indicates per interface how long (in hours, minutes, and seconds) the entry has been in the IPv6 multicast routing table. “Expires” indicates per interface how long (in hours, minutes, and seconds) until the entry will be removed from the IPv6 multicast routing table.

Table 200 show ipv6 mroute Field Descriptions (continued)

Field	Description
Interface state:	Indicates the state of the incoming or outgoing interface. • Interface. Indicates the type and number of the interface listed in the incoming or outgoing interface list. • Next-Hop. "Next-Hop" specifies the IP address of the downstream neighbor. • State/Mode. "State" indicates that packets will either be forwarded, pruned, or null on the interface depending on whether there are restrictions due to access lists. "Mode" indicates that the interface is operating in sparse mode.
(*, FF07::1) and (2001:0DB8:999::99)	Entry in the IPv6 multicast routing table. The entry consists of the IPv6 address of the source router followed by the IPv6 address of the multicast group. An asterisk (*) in place of the source router indicates all sources. Entries in the first format are referred to as (*, G) or "star comma G" entries. Entries in the second format are referred to as (S, G) or "S comma G" entries; (*, G) entries are used to build (S, G) entries.
RP	Address of the RP router.
flags:	Information set by the MRIB clients on this MRIB entry.
Incoming interface:	Expected interface for a multicast packet from the source. If the packet is not received on this interface, it is discarded.
RPF nbr	IP address of the upstream router to the RP or source.
Outgoing interface list:	Interfaces through which packets will be forwarded. For (S,G) entries, this list will not include the interfaces inherited from the (*,G) entry.

Related Commands

Command	Description
ipv6 multicast-routing	Enables multicast routing using PIM and MLD on all IPv6-enabled interfaces of the router and enables multicast forwarding.
show ipv6 mfib	Displays the forwarding entries and interfaces in the IPv6 MFIB.

show ipv6 mroute active

To display the active multicast streams on the router, use the **show ipv6 mroute active** command in user EXEC or privileged EXEC mode.

show ipv6 mroute [**vrf** *vrf-name*] [**link-local** | *group-name* | *group-address*] **active** [*kbps*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
link-local	(Optional) Displays the link-local groups.
group-name | *group-address*	(Optional) IPv6 address or name of the multicast group.
kbps	(Optional) Displays the rate that active sources are sending to multicast groups. Active sources are those sending at the kbps value or higher. The *kbps* argument defaults to 4 kbps.

Command Default

The *kbps* argument defaults to 4 kbps.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	The **link-local** keyword was added.
12.3(4)T	The **link-local** keyword was added.
12.2(25)S	The **link-local** 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.
12.2(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.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

The **show ipv6 mroute active** command displays active multicast streams with data rates that are greater than or equal to the kilobits per second set by the user. The command default is 4 kbps.

Examples

The following is sample output from the **show ipv6 mroute active** command:

```
Router# show ipv6 mroute active

Active IPv6 Multicast Sources - sending >= 4 kbps
```

```
Group:FF05::1
 Source:2001::1:1:1
   Rate:11 pps/8 kbps(1sec), 8 kbps(last 8 sec)
```

Table 201 describes the significant fields shown in the display.

Table 201 show ipv6 mroute active Field Descriptions

Field	Description
Group:	Summary information about counters for (*, G) and the range of (S, G) states for one particular group G. The following RP-tree: and Source: output fields contain information about the individual states belonging to this group. **Note** For Source Specific Multicast (PIM-SSM) range groups, the Group: displays are statistical. All SSM range (S, G) states are individual, unrelated SSM channels.
Rate...kbps	Bytes per second divided by packets per second divided by 1000. On an IP multicast fast-switching platform, the number of packets per second is the number of packets during the last second. Other platforms may use a different approach to calculate this number. Please refer to the platform documentation for more information.

show ipv6 mtu

To display maximum transmission unit (MTU) cache information for IPv6 interfaces, use the **show ipv6 mtu** command in user EXEC or privileged EXEC mode.

show ipv6 mtu [**vrf** *vrfname*]

Syntax Description

vrf	(Optional) Displays an IPv6 Virtual Private Network (VPN) routing/forwarding instance (VRF).
vrfname	(Optional) Name of the IPv6 VRF.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(2)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 Release 12.2(14)S.
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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SB	The **vrf** keyword and *vrfname* argument were added.

Usage Guidelines

The **vrf** keyword and *vrfname* argument allow you to view MTUs related to a specific VRF.

Examples

The following is sample output from the **show ipv6 mtu** command:

```
Router# show ipv6 mtu

MTU     Since    Destination Address
1400    00:04:21  5000:1::3
1280    00:04:50  FE80::203:A0FF:FED6:141D
```

The following is sample output from the **show ipv6 mtu** command using the **vrf** keyword and *vrfname* argument. This example provides information about the VRF named vrfname1:

```
Router# show ipv6 mtu vrf vrfname1

MTU   Since       Source Address     Destination Address
1300  00:00:04    2001:0DB8:2        2001:0DB8:7
```

Table 202 describes the significant fields shown in the display.

Table 202 show ipv6 mtu Field Descriptions

Field	Description
MTU	MTU, which was contained in the Internet Control Message Protocol (ICMP) packet-too-big message, used for the path to the destination address.
Since	Age of the entry since the ICMP packet-too-big message was received.
Destination Address	Address contained in the received ICMP packet-too-big message. Packets originating from this router to this address should be no bigger than the given MTU.

Related Commands

Command	Description
ipv6 mtu	Sets the MTU size of IPv6 packets sent on an interface.

show ipv6 nat statistics

To display Network Address Translation—Protocol Translation (NAT-PT) statistics, use the **show iv6 nat statistics** command in user EXEC or privileged EXEC mode.

show ipv6 nat statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(13)T	This command was introduced.

Examples

The following is sample output from the **show ipv6 nat statistics** command:

```
Router# show ipv6 nat statistics

Total active translations: 4 (2 static, 2 dynamic; 2 extended)
NAT-PT interfaces:
  Ethernet3/1, Ethernet3/3
Hits: 1  Misses: 1
Expired translations: 0
```

Table 203 describes the significant fields shown in the display.

Table 203 show ipv6 nat statistics Field Descriptions

Field	Description
Total active translations	Number of translations active in the system. This number increments by one each time a translation is created and is decremented each time a translation is cleared or times out. Displays the numbers for each type of translation.
NAT-PT interfaces	The interfaces, by type and number, that are configured to run NAT-PT translations.
Hits	Number of times the software does a translations table lookup and finds an entry.
Misses	Number of times the software does a translations table lookup, fails to find an entry, and must try to create one.
Expired translations	Cumulative count of translations that have expired since the router was booted.

Related Commands

Command	Description
show ipv6 nat translations	Displays active NAT-PT translations.

show ipv6 nat translations

To display active Network Address Translation—Protocol Translation (NAT-PT) translations, use the **show ip nat translations** command in user EXEC or privileged EXEC mode.

show ipv6 nat translations [**icmp** | **tcp** | **udp**] [**verbose**]

Syntax Description

icmp	(Optional) Displays detailed information about NAT-PT ICMP translation events.
tcp	(Optional) Displays detailed information about NAT-PT TCP translation events.
udp	(Optional) Displays detailed information about NAT-PT User Datagram Protocol (UDP) translation events.
verbose	(Optional) Displays additional information for each translation table entry, including how long ago the entry was created and used.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(13)T	This command was introduced.

Examples

The following is sample output from the **show ip nat translations** command. Two static translations have been configured between an IPv4 source address and an IPv6 destination, and vice versa.

```
Router# show ipv6 nat translations

Prot  IPv4 source              IPv6 source
      IPv4 destination         IPv6 destination
---   ---                      ---
      192.168.123.2            2001::2

---   ---                      ---
      192.168.122.10           2001::10

tcp   192.168.124.8,11047      3002::8,11047
      192.168.123.2,23         2001::2,23

udp   192.168.124.8,52922      3002::8,52922
      192.168.123.2,69         2001::2,69

udp   192.168.124.8,52922      3002::8,52922
      192.168.123.2,52922      2001::2,52922

---   192.168.124.8            3002::8
      192.168.123.2            2001::2
```

```
---   192.168.124.8           3002::8
      ---                     ---

---   192.168.121.4           5001::4
      ---                     ---
```

The following is sample output that includes the **verbose** keyword:

```
Router# show ipv6 nat translations verbose

Prot  IPv4 source             IPv6 source
      IPv4 destination        IPv6 destination
---   ---                     ---
      192.168.123.2           2001::2
      create 00:04:24, use 00:03:24,

---   ---                     ---
      192.168.122.10          2001::10
      create 00:04:24, use 00:04:24,

tcp   192.168.124.8,11047     3002::8,11047
      192.168.123.2,23        2001::2,23
      create 00:03:24, use 00:03:20, left 00:16:39,

udp   192.168.124.8,52922     3002::8,52922
      192.168.123.2,69        2001::2,69
      create 00:02:51, use 00:02:37, left 00:17:22,

udp   192.168.124.8,52922     3002::8,52922
      192.168.123.2,52922     2001::2,52922
      create 00:02:48, use 00:02:30, left 00:17:29,

---   192.168.124.8           3002::8
      192.168.123.2           2001::2
      create 00:03:24, use 00:02:34, left 00:17:25,

---   192.168.124.8           3002::8
      ---                     ---
      create 00:04:24, use 00:03:24,

---   192.168.121.4           5001::4
      ---                     ---
      create 00:04:25, use 00:04:25,
```

Table 204 describes the significant fields shown in the display.

Table 204 show ipv6 nat translations Field Descriptions

Field	Description
Prot	Protocol of the port identifying the address.
IPv4 source/IPv6 source	The IPv4 or IPv6 source address to be translated.
IPv4 destination/IPv6 destination	The IPv4 or IPv6 destination address.
create	How long ago the entry was created (in hours:minutes:seconds).
use	How long ago the entry was last used (in hours:minutes:seconds).
left	Time before the entry times out (in hours:minutes:seconds).

Related Commands

Command	Description
clear ipv6 nat translation	Clears dynamic NAT-PT translations from the translation state table.

show ipv6 nd raguard counters

To display information about RA guard counters, use the **show ipv6 nd raguard policy** command in privileged EXEC mode.

show ipv6 nd raguard counters [**interface** *type number*]

Syntax Description

interface *type number*	(Optional) Displays RA guard policy information for the specified interface type and number.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(5th)SXI	This command was introduced.

Usage Guidelines

The **show ipv6 nd raguard counters** command displays information about RA guard counters, such as packets sent, packets received, and packets droped. This command also provides information on why a packet was dropped.

show ipv6 nd raguard policy

To display router advertisements (RAs) guard policy on all interfaces configured with RA guard, use the **show ipv6 nd raguard policy** command in privileged EXEC mode.

show ipv6 nd raguard policy [**interface** *type number*]

Syntax Description

interface *type number*	(Optional) Displays RA guard policy information for the specified interface type and number.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

The **show ipv6 nd raguard policy** command hows the options configured for the policy on interfaces where the feature is enabled.

Examples

The following example shows the policy configuration for a policy named raguard1, as well as all the interfaces where the policy is applied:

```
Router# show ipv6 nd raguard policy raguard1

Policy raguard1 configuration:
  device-role host

Policy applied on the following interfaces:

  Et0/0        vlan all
  Et1/0        vlan all
```

Table 205 describes the significant fields shown in the display.

Table 205 show ipv6 nd raguard policy Field Descriptions

Field	Description
Policy raguard1 configuration:	Configuration of the specified policy.
device-role host	The role of the device attached to the port. This device configuration is that of host.
Policy applied on the following interfaces:	The specified interface on which RA guard is configured.

show ipv6 neighbor binding

To display contents of a binding table, use the **show ipv6 neighbor binding** command in privileged EXEC mode.

show ipv6 neighbor binding [**vlan** *vlan-id* | **interface** *type number* | **ipv6** *ipv6-address* | **mac** *mac-address*]

Syntax Description

vlan *vlan-id*	(Optional) Displays the binding table entries that match the specified VLAN.
interface *type number*	(Optional) Displays the binding table entries that match the specified interface type and number.
ipv6 *ipv6-address*	(Optional) Displays the binding table entries that match the specified IPv6 address.
mac *mac-address*	(Optional) Displays the binding table entries that match the specified Media Access Control (MAC) address.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

The **show ipv6 neighbor binding** command displays the contents of the binding table. The display output can be specified by the specified VLAN, interface, IPv6 address, or MAC address. If no keywords or arguments are entered, all binding table contents are displayed.

The following keyword and argument combinations are allowed:

- **vlan** *vlan-id*: Displays all entries for the specified VLAN
- **interface** *type number*: Displays all entries for the specified interface
- **ipv6** *ipv6-address* + **interface** *type number* + **vlan** *vlan-id*: Displays a single entry that matches these three keyword and argument combinations
- **ipv6** *ipv6-address* + **interface** *type number*: Displays all entries for the specified IPv6 address and interface.
- **ipv6** *ipv6-address*: Displays all entries for the specified IPv6 address.

Examples

The following example displays the contents of a binding table:

```
Router# show ipv6 neighbor binding

address DB has 4 entries
Codes: L - Local, S - Static, ND - Neighbor Discovery
Preflevel (prlvl) values:
1:Not secure          2:MAC and LLA match   3:Cga authenticated
4:Dhcp assigned       5:Cert authenticated  6:Cga and Cert auth
7:Trusted port        8:Statically assigned
```

```
    IPv6 address            Link-Layer addr Interface   vlan  prlvl age state    Time left
ND  FE80::A8BB:CCFF:FE01:F500  AABB.CC01.F500  Et0/0     100  0002    0 REACHABLE  8850
L   FE80::21D:71FF:FE99:4900   001D.7199.4900  Vl100     100  0080 7203 DOWN       N/A
ND  2001:600::1                AABB.CC01.F500  Et0/0     100  0003    0 REACHABLE  3181
ND  2001:300::1                AABB.CC01.F500  Et0/0     100  0007    0 REACHABLE  9559
ND  2001:100::2                AABB.CC01.F600  Et1/0     200  0002    0 REACHABLE  9196
L   2001:400::1                001D.7199.4900  Vl100     100  0080 7188 DOWN       N/A
S   2001:500::1                000A.000B.000C  Fa4/13    300  0080 8676 STALE      N/A
```

Table 205 describes the significant fields shown in the display.

Table 206 show ipv6 neighbor binding Field Descriptions

Field	Description
address DB has 4 entries	Number of entries in the specified database.

Related Commands

Command	Description
ipv6 neighbor binding	Changes the defaults of neighbor binding entries in a binding table.

show ipv6 snooping capture-policy

To display message capture policies, use the **show ipv6 snooping capture-policy** command in user EXEC or privileged EXEC mode.

show ipv6 snooping capture-policy [**interface** *type number*]

Syntax Description

interface *type number*	(Optional) Displays first-hop message types on the specified interface type and number.

Command Modes

User EXEC
Privileged EXEC (#)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

The **show ipv6 snooping capture-policy** command displays IPv6 first-hop message capture policies.

Examples

The following example shows **show ipv6 snooping capture-policy** command output on the Ethernet 0/0 interface, on which the IPv6 Neighbor Discovery Protocol (NDP) inspection and Router Advertisement (RA) Guard features are configured:

```
Router# show ipv6 snooping capture-policy

Hardware policy registered on Et0/0
Protocol  Protocol value  Message  Value  Action  Feature
ICMP      58              RS       85     punt    RA Guard
                                          punt    ND Inspection
ICMP      58              RA       86     drop    RA guard
                                          punt    ND Inspection
ICMP      58              NS       87     punt    ND Inspection
ICMP      58              NA       88     punt    ND Inspection
ICMP      58              REDIR    89     drop    RA Guard
                                          punt    ND Inspection
```

Table 205 describes the significant fields shown in the display.

Table 207 show ipv6 snooping capture-policy Field Descriptions

Field	Description
Hardware policy registered on Fa4/11	A hardware policy contains a programmatic access list (ACL), with a list of access control entries (ACEs).
Protocol	The protocol whose packets are being inspected.
Message	The type of message being inspected.

Table 207 show ipv6 snooping capture-policy Field Descriptions (continued)

Field	Description
Action	Action to be taken on the packet.
Feature	The inspection feature for this information.

show ipv6 snooping counters

To display information about the packets counted by the interface counter, use the **show ipv6 snooping counters** command in user EXEC or privileged EXEC mode.

show ipv6 snooping counters [**interface** *type number*]

Syntax Description

interface *type number*	(Optional) Displays first hop packets that match the specified interface type and number.

Command Modes

User EXEC
Privileged EXEC (#)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

The **show ipv6 snooping counters** command shows packets handled by the switcher that are being counted in interface counters. The switcher counts packets captured per interface and records whether the packet was received, sent, or dropped. If a packet is dropped, the reason for the drop and the feature that caused the drop are both also provided.

Examples

The following examples shows information about packets counted on interface FastEthernet4/12:

```
Router# show ipv6 snooping counters interface Fa4/12

Received messages on Fa4/12:
Protocol        Protocol message
ICMPv6          RS      RA      NS      NA      REDIR   CPS     CPA
                0       4256    0       0       0       0       0

Bridged messages from Fa4/12:
Protocol        Protocol message
ICMPv6          RS      RA      NS      NA      REDIR   CPS     CPA
                0       4240    0       0       0       0       0

Dropped messages on Fa4/12:
Feature/Message RS      RA      NS      NA      REDIR   CPS     CPA
RA guard        0       16      0       0       0       0       0

Dropped reasons on Fa4/12:
RA guard         16   RA drop - reason:RA/REDIR received on un-authorized port
```

Table 205 describes the significant fields shown in the display:

Table 208 show ipv6 snooping counters Field Descriptions

Field	Description
Received messages on Fa4/12:	The messages received on an interface.
Protocol	The protocol for which messages are being counted.
Protocol message	The type of protocol messages being counted.
Bridged messages from Fa4/12:	Bridged messages from the interface.
Dropped messages an Fa4/12:	The messages dropped on the interface.
Feature/message	The feature that caused the drop, and the type and number of messages dropped.
RA drop - reason:RA/REDIR received on un-authorized port	The reason these messages were dropped.

show ipv6 snooping features

To display information about about snooping features configured on the router, use the **show ipv6 snooping features** command in user EXEC or privileged EXEC mode.

show ipv6 snooping features

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC (#)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

The **show ipv6 snooping features** command shows the first hop features that are configured on the router.

Examples

The following example shows that both IPv6 ND inspection and IPv6 RA Guard are configured on the router:

```
Router# show ipv6 snooping features

Feature name   priority state
RA guard          100   READY
NDP inspection     20   READY
```

Table 205 describes the significant fields shown in the display.

Table 209 show ipv6 snooping features Field Descriptions

Field	Description
Feature name	The names of the IPv6 global policy features configured on the router.
Priority	The priority of the specified feature.
State	The state of the specified feature.

show ipv6 nd raguard policy

To display router advertisements (RAs) guard policy on all interfaces configured with RA guard, use the **show ipv6 nd raguard policy** command in privileged EXEC mode.

show ipv6 nd raguard policy [**interface** *type number*]

Syntax Description

interface *type number*	(Optional) Displays RA guard policy information for the specified interface type and number.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

The **show ipv6 nd raguard policy** command hows the options configured for the policy on interfaces where the feature is enabled.

Examples

The following example shows the policy configuration for a policy named raguard1, as well as all the interfaces where the policy is applied:

```
Router# show ipv6 nd raguard policy raguard1

Policy raguard1 configuration:
  device-role host

Policy applied on the following interfaces:

  Et0/0        vlan all
  Et1/0        vlan all
```

Table 205 describes the significant fields shown in the display.

Table 210 show ipv6 nd raguard policy Field Descriptions

Field	Description
Policy raguard1 configuration:	Configuration of the specified policy.
device-role host	The role of the device attached to the port. This device configuration is that of host.
Policy applied on the following interfaces:	The specified interface on which RA guard is configured.

show ipv6 nd secured certificates

To display active IPv6 Secure Neighbor Discovery (SeND) certificates, use the **show ipv6 nd secured certificates** command in privileged EXEC mode.

show ipv6 nd secured certificates

Syntax Description

This command has no arguments or keywords.

Command Default

No SeND certificates are displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

The **show ipv6 nd secured certificates** command is used on hosts (routers configured in host mode) to display the certifcates received over SeND (via Certificate Path Advertisement) and their state.

Examples

The following example displays active SeND certificates:

```
Router# show ipv6 nd secured certificates

Total number of entries: 1 / 32

Hash                             id         RA  certcnt certrcv state
DC0102E09FAF422D49ED79A846D2EBC1 0x00000778 no  1       1       CERT_VALIDATED
certificate No 0
subject  hostname=sa14-72a,c=FR,st=fr,l=example,o=cisco,ou=nsstg,cn=72a
issuer  c=FR,st=fr,l=example,o=cisco,ou=nsstg,cn=CA0
```

Table 205 describes the significant fields shown in the display.

Table 211 show ipv6 nd secured certificates Field Descriptions

Field	Description
certcnt	Number of certificate for this chain.
certrcv	Number of certifciate received in the chain.
Hash	Key hash.
id	Numero of the certifciate.
RA	Displays Yes if an RA is pending for this certifciate.
state	Current state of the certificate.

Related Commands

Command	Description
show ipv6 cga modifier-db	Displays IPv6 CGA modifiers.
show ipv6 cga address-db	Displays IPv6 CGAs.
show ipv6 nd secured counters interface	Displays SeND counters on an interface.
show ipv6 nd secured nonce-db	Displays active SeND nonce entries.
show ipv6 nd secured timestamp-db	Displays active SeND time-stamp entries.

show ipv6 nd secured counters interface

To display IPv6 Secure Neighbor Discovery (SeND) counters on an interface, use the **show ipv6 nd secured counters interface** command in privileged EXEC mode.

show ipv6 nd secured counters interface *interface*

Syntax Description

interface	(Optional) Specifies the interface on which SeND counters are located.

Command Default

No SeND counter information is displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(24)T	This command was introduced.

Examples

The following example displays SeND counters:

```
Router# show ipv6 nd secured counters interface ethernet0/0

e0/0 Received ND messages on Ethernet0/0:
rcvd    accept  SLLA    TLLA    PREFIX  MTU     CGA     RSA     TS      NONCE   TA CERT
RA      66      65      63      0       62      63      63      63      63      0       0
0
NS      8       8       8       0       0       0       8       8       8       8       0
0
NA      20      20      0       8       0       0       19      19      19      14      0
0
CPA     1       1       0       0       0       0       0       0       0       0       1
1
Dropped ND messages on Ethernet0/0:
Codes   TIMEOUT: Timed out while waiting for rsp

        drop    TIMEOUT
RA      1       1
Sent ND messages on Ethernet0/0:
sent    aborted SLLA    CGA     RSA     TS      NONCE   TA
NS      14      0       14      14      14      14      14      0
NA      8       0       0       8       8       8       8       0
CPS     43      0       0       0       0       0       0       43
Router#
```

Table 205 describes the significant fields shown in the display.

Table 212 show ipv6 nd secured counters interface Field Descriptions

Field	Description
accept	Number of neighbor discovery (ND) messages accepted (messages that are not dropped).
CERT	Number of messages received with the certificate option.
CGA	Number of messages received with the CGA option.
MTU	Number of messages received with the MTU option.
NA	Number of NDP neighbor advertisements
NONCE	Number of messages received with the NONCE option.
NS	Number of NDP neighbor solicitions.
PREFIX	Number of messages received with the PREFIX option.
rcvd	Number of ND messages received on the interface.
RA	Number of router advertisements.
REDIR	Number of NDP redirect messages.
RS	Router Solicit.
RSA	Number of messages received with the RSA option.
SLLA	Number of messages received with the ND SLLA option.
TA	Number of messages received with the trust anchor option.
TS	Number of messages received with the time stamp option.

Related Commands

Command	Description
show ipv6 cga address-db	Displays IPv6 CGAs.
show ipv6 cga modifier-db	Displays IPv6 CGA modifiers.
show ipv6 nd secured certificates	Displays active SeND certificates.
show ipv6 nd secured nonce-db	Displays active SeND nonce entries.
show ipv6 nd secured timestamp-db	Displays active SeND timestamp entries.

show ipv6 nd secured nonce-db

To display active IPv6 Secure Neighbor Discovery (SeND) nonce database entries, use the **show ipv6 nd secured nonce-db** command in privileged EXEC mode.

show ipv6 nd secured nonce-db

Syntax Description

This command has no arguments or keywords.

Command Default

No SeND nonce information is displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

The **show ipv6 nd secured nonce-db** command is used to display the pending solicitations. There are rarely any pending solicitations because the solicitations are quickly answered and removed from the database.

Examples

The following example displays active SeND nonce entries. The output is self-explanatory.

```
Router# show ipv6 nd secured nonce-db

Total number of entries: 0
```

Related Commands

Command	Description
show ipv6 cga address-db	Displays IPv6 CGAs.
show ipv6 cga modifier-db	Displays IPv6 CGA modifiers.
show ipv6 nd secured certificates	Displays active SeND certificates.
show ipv6 nd secured counters interface	Displays SeND counters on an interface.
show ipv6 nd secured timestamp-db	Displays active SeND time stamp entries.

show ipv6 nd secured solicit-db

To display pending SEcure Neighbor Discovery (SEND) solicitations from peers, use the **show ipv6 nd secured solicit-db** command in privileged EXEC configuration mode.

show ipv6 nd secured solicit-db

Syntax Description

This command has no arguments or keywords.

Command Default

No pending SEND solicitation information is displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

Use this command to display pending SEND solicitations.

Examples

The following example displays pending SEcure Neighbor Discovery (SEND) solicitations from peers:

```
Router# show ipv6 nd secured solicit-db
```

show ipv6 nd secured timestamp-db

To display active Secure Neighbor Discovery (SeND) time-stamp database entries, use the **show ipv6 nd secured timestamp-db** command in privileged EXEC mode.

show ipv6 nd secured timestamp-db

Syntax Description

This command has no arguments or keywords.

Command Default

No pending SeND solicitation information is displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

The **show ipv6 nd secured timestamp-db** command displays the content of the time-stamp databse, which contains last received messages from peers. It also displays the delta and fuzz values.

Examples

The following example displays active SeND time-stamp database entries:

```
Router# show ipv6 nd secured timestamp-db

Total number of entries: 6 Number of unreached peer entries: 3 / 1024
FE80::289C:3308:4719:87F2 on Ethernet0/0, delta 300s, fuzz 1000ms
        Time to expire: 3h 41m 16s (reached)
        TSlast: 0x4936B97655FF = Wed Dec  3 16:53:10 2008
        RDlast: 0x4936B976438B = Wed Dec  3 16:53:10 2008
FE80::2441:88D1:22FC:3B77 on Ethernet0/0, delta 300s, fuzz 1000ms
        Time to expire: 3h 59m 53s (reached)
        TSlast: 0x4936BDD2E13E = Wed Dec  3 17:11:46 2008
        RDlast: 0x4936BDD2D0D6 = Wed Dec  3 17:11:46 2008
FE80::E2:F012:6F72:9E45 on Ethernet0/0, delta 300s, fuzz 1000ms
        Time to expire: 3h 4m 18s (unreached)
        TSlast: 0x4936B0CBB333 = Wed Dec  3 16:16:11 2008
       RDlast: 0x4936B0CBBD70 = Wed Dec  3 16:16:11 2008 2001:100::38C9:4A1A:2972:794E on
Ethernet0/0, delta 300s, fuzz 1000ms
        Time to expire: 3h 4m 19s (unreached)
        TSlast: 0x4936BA254FDA = Wed Dec  3 16:56:05 2008
        RDlast: 0x4936BA253F72 = Wed Dec  3 16:56:05 2008 2001:100::383E:6BD5:397:4A50 on
Ethernet0/0, delta 300s, fuzz 1000ms
        Time to expire: 3h 45m 0s (reached)
        TSlast: 0x4936BA55F2AA = Wed Dec  3 16:56:53 2008
        RDlast: 0x4936BA55E036 = Wed Dec  3 16:56:53 2008
2001:100::434:E62D:327D:B1E6 on Ethernet0/0, delta 300s, fuzz 1000ms
        Time to expire: 3h 4m 42s (unreached)
        TSlast: 0x4936B0E422D0 = Wed Dec  3 16:16:36 2008
        RDlast: 0x4936B0E42D0E = Wed Dec  3 16:16:36 2008
```

Table 213 describes the significant fields shown in the display.

Table 213 show ipv6 nd secured timestamp-db Field Descriptions

Field	Description
Total number of entries	Number of entries (peers) in the cache.
Time to expire	Remaining time before entry expires.
TSlast	Last peer timestamp value.
RDlast	Time when the last message was received from the peer.

Related Commands

Command	Description
show ipv6 cga address-db	Displays IPv6 CGAs.
show ipv6 cga modifier-db	Displays IPv6 CGA modifiers.
show ipv6 nd secured certificates	Displays active SeND certificates.
show ipv6 nd secured counters interface	Displays SeND counters on an interface.
show ipv6 nd secured nonce-db	Displays active SeND nonce entries.

show ipv6 neighbor binding

To display contents of a binding table, use the **show ipv6 neighbor binding** command in privileged EXEC mode.

show ipv6 neighbor binding [**vlan** *vlan-id* | **interface** *type number* | **ipv6** *ipv6-address* | **mac** *mac-address*]

Syntax Description

vlan *vlan-id*	(Optional) Displays the binding table entries that match the specified VLAN.
interface *type number*	(Optional) Displays the binding table entries that match the specified interface type and number.
ipv6 *ipv6-address*	(Optional) Displays the binding table entries that match the specified IPv6 address.
mac *mac-address*	(Optional) Displays the binding table entries that match the specified Media Access Control (MAC) address.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

The **show ipv6 neighbor binding** command displays the contents of the binding table. The display output can be specified by the specified VLAN, interface, IPv6 address, or MAC address. If no keywords or arguments are entered, all binding table contents are displayed.

The following keyword and argument combinations are allowed:

- **vlan** *vlan-id*: Displays all entries for the specified VLAN
- **interface** *type number*: Displays all entries for the specified interface
- **ipv6** *ipv6-address* + **interface** *type number* + **vlan** *vlan-id*: Displays a single entry that matches these three keyword and argument combinations
- **ipv6** *ipv6-address* + **interface** *type number*: Displays all entries for the specified IPv6 address and interface.
- **ipv6** *ipv6-address*: Displays all entries for the specified IPv6 address.

Examples

The following example displays the contents of a binding table:

```
Router# show ipv6 neighbor binding

address DB has 4 entries
Codes: L - Local, S - Static, ND - Neighbor Discovery
Preflevel (prlvl) values:
1:Not secure          2:MAC and LLA match   3:Cga authenticated
4:Dhcp assigned       5:Cert authenticated  6:Cga and Cert auth
7:Trusted port        8:Statically assigned
```

```
    IPv6 address            Link-Layer addr Interface   vlan  prlvl age state    Time left
ND  FE80::A8BB:CCFF:FE01:F500  AABB.CC01.F500  Et0/0     100  0002    0 REACHABLE  8850
L   FE80::21D:71FF:FE99:4900   001D.7199.4900  Vl100     100  0080 7203 DOWN       N/A
ND  2001:600::1                AABB.CC01.F500  Et0/0     100  0003    0 REACHABLE  3181
ND  2001:300::1                AABB.CC01.F500  Et0/0     100  0007    0 REACHABLE  9559
ND  2001:100::2                AABB.CC01.F600  Et1/0     200  0002    0 REACHABLE  9196
L   2001:400::1                001D.7199.4900  Vl100     100  0080 7188 DOWN       N/A
S   2001:500::1                000A.000B.000C  Fa4/13    300  0080 8676 STALE      N/A
```

Table 205 describes the significant fields shown in the display.

Table 214 show ipv6 neighbor binding Field Descriptions

Field	Description
address DB has 4 entries	Number of entries in the specified database.
Codes	

Related Commands

Command	Description
ipv6 neighbor binding	Changes the defaults of neighbor binding entries in a binding table.

show ipv6 neighbors

To display IPv6 neighbor discovery (ND) cache information, use the **show ipv6 neighbors** command in user EXEC or privileged EXEC mode.

show ipv6 neighbors [*interface-type interface-number* | *ipv6-address* | *ipv6-hostname* | **statistics**]

Syntax Description

interface-type	(Optional) Specifies the type of the interface from which IPv6 neighbor information is to be displayed.
interface-number	(Optional) Specifies the number of the interface from which IPv6 neighbor information is to be displayed.
ipv6-address	(Optional) Specifies the IPv6 address of the neighbor. 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-hostname	(Optional) Specifies the IPv6 hostname of the remote networking device.
statistics	(Optional) Displays ND cache statistics.

Command Default

All IPv6 ND cache entries are listed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(8)T	This command was modified. Support for static entries in the IPv6 neighbor discovery cache was added to the command output.
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 Release 12.2(14)S.
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.
12.2(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 and introduced on Cisco ASR 1000 Series Routers.
Cisco IOS XE Release 2.6	This command was modified. This command was updated to display the number and the limit of ND cache entries on a particular interface.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T.

Usage Guidelines

When the *interface-type* and *interface-number* arguments are not specified, cache information for all IPv6 neighbors is displayed. Specifying the *interface-type* and *interface-number* arguments displays only cache information about the specified interface.

Specifying the **statistics** keyword displays ND cache statistics.

Examples

The following is sample output from the **show ipv6 neighbors** command when entered with an interface type and number:

```
Router# show ipv6 neighbors ethernet 2

IPv6 Address                              Age Link-layer Addr State Interface
2000:0:0:4::2                               0 0003.a0d6.141e  REACH Ethernet2
FE80::203:A0FF:FED6:141E                    0 0003.a0d6.141e  REACH Ethernet2
3001:1::45a                                 - 0002.7d1a.9472  REACH Ethernet2
```

The following is sample output from the **show ipv6 neighbors** command when entered with an IPv6 address:

```
Router# show ipv6 neighbors 2000:0:0:4::2

IPv6 Address                              Age Link-layer Addr State Interface
2000:0:0:4::2                               0 0003.a0d6.141e  REACH Ethernet2
```

Table 215 describes the significant fields shown in the displays.

Table 215 show ipv6 neighbors Field Descriptions

Field	Description
IPv6 Address	IPv6 address of neighbor or interface.
Age	Time (in minutes) since the address was confirmed to be reachable. A hyphen (-) indicates a static entry.
Link-layer Addr	MAC address. If the address is unknown, a hyphen (-) is displayed.

Table 215 show ipv6 neighbors Field Descriptions (continued)

Field	Description
State	The state of the neighbor cache entry. Following are the states for dynamic entries in the IPv6 neighbor discovery cache: • INCMP (Incomplete)—Address resolution is being performed on the entry. A neighbor solicitation message has been sent to the solicited-node multicast address of the target, but the corresponding neighbor advertisement message has not yet been received. • REACH (Reachable)—Positive confirmation was received within the last ReachableTime milliseconds that the forward path to the neighbor was functioning properly. While in REACH state, the device takes no special action as packets are sent. • STALE—More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that the forward path was functioning properly. While in STALE state, the device takes no action until a packet is sent. • DELAY—More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that the forward path was functioning properly. A packet was sent within the last DELAY_FIRST_PROBE_TIME seconds. If no reachability confirmation is received within DELAY_FIRST_PROBE_TIME seconds of entering the DELAY state, send a neighbor solicitation message and change the state to PROBE. • PROBE—A reachability confirmation is actively sought by resending neighbor solicitation messages every RetransTimer milliseconds until a reachability confirmation is received. • ????—Unknown state. Following are the possible states for static entries in the IPv6 neighbor discovery cache: • INCMP (Incomplete)—The interface for this entry is down. • REACH (Reachable)—The interface for this entry is up. **Note** Reachability detection is not applied to static entries in the IPv6 neighbor discovery cache; therefore, the descriptions for the INCMP (Incomplete) and REACH (Reachable) states are different for dynamic and static cache entries.
Interface	Interface from which the address was reachable.

The following is sample output from the **show ipv6 neighbors** command with the **statistics** keyword:

```
Router# show ipv6 neighbor statistics

IPv6 ND Statistics
 Entries 2, High-water 2, Gleaned 1, Scavenged 0
 Entry States
   INCMP 0  REACH 0  STALE 2  GLEAN 0  DELAY 0  PROBE 0
 Resolutions (INCMP)
   Requested 1, timeouts 0, resolved 1, failed 0
   In-progress 0, High-water 1, Throttled 0, Data discards 0
 Resolutions (PROBE)
```

```
Requested 3, timeouts 0, resolved 3, failed 0
```

Table 216 describes the significant fields shown in this display:

Table 216 show ipv6 neighbors statistics Field Descriptions

Field	Description
Entries	Total number of ND neighbor entries in the ND cache.
High-Water	Maximum amount (so far) of ND neighbor entries in ND cache.
Gleaned	Number of ND neighbor entries gleaned (that is, learned from a neighbor NA or other ND packet).
Scavenged	Number of stale ND neighbor entries that have timed out and been removed from the cache.
Entry States[1]	Number of ND neighbor entries in each state.
Resolutions (INCMP)	Statistics for neighbor resolutions attempted in INCMP state[1] (that is, resolutions prompted by a data packet). Details about the resolutions attempted in INCMP state are follows: • Requested—Total number of resolutions requested. • Timeouts—Number of timeouts during resolutions. • Resolved—Number of successful resolutions. • Failed—Number of unsuccessful resolutions. • In-progress—Number of resolutions in progress. • High-water—Maximum number (so far) of resolutions in progress. • Throttled—Number of times resolution request was ignored due to maximum number of resolutions in progress limit. • Data discards—Number of data packets discarded that are awaiting neighbor resolution.
Resolutions (PROBE)	Statistics for neighbor resolutions attempted in PROBE state (that is, re-resolutions of existing entries prompted by a data packet): • Requested—Total number of resolutions requested. • Timeouts—Number of timeouts during resolutions. • Resolved—Number of successful resolutions. • Failed—Number of unsuccessful resolutions.

1. Reachability detection is not applied to static entries in the IPv6 neighbor discovery cache. A static entry is always in the REACH (Reachable) state unless the associated interface is down or IPv6 is not enabled on the interface.

The following example shows the ND cache limit on port-channel 1.11:

```
Router# show ipv6 neighbor port-channel1.11

Interface Port-channel1.11, entries 4, static 0, limit 4, ignored 0

IPv6 Address                     Age  Link-layer Addr  State   Interface
2001:2::93                       0    aabb.cc00.5d02   REACH   Po1.11
FE80::A8BB:CCFF:FE00:5D02        0    aabb.cc00.5d02   DELAY   Po1.11
2001:2::92                       0    aabb.cc00.5d01   STALE   Po1.11
2001:2::95                       0    aabb.cc00.5d01   STALE   Po1.11
```

show ipv6 nhrp

To display Next Hop Resolution Protocol (NHRP) mapping information, use the **show ipv6 nhrp** command in user EXEC or privileged EXEC mode.

show ipv6 nhrp [**dynamic** [*ipv6-address*] | **incomplete** | **static**] [*address* | *interface*] [**brief** | **detail**] [**purge**]

Syntax Description

dynamic	(Optional) Displays dynamic (learned) IPv6-to-nonbroadcast multiaccess address (NBMA) mapping entries. Dynamic NHRP mapping entries are obtained from NHRP resolution/registration exchanges. See Table 217 for types, number ranges, and descriptions.
ipv6-address	(Optional) The IPv6 address of the cache entry.
incomplete	(Optional) Displays information about NHRP mapping entries for which the IPv6-to-NBMA is not resolved. See Table 217 for types, number ranges, and descriptions.
static	(Optional) Displays static IPv6-to-NBMA address mapping entries. Static NHRP mapping entries are configured using the **ipv6 nhrp map** command. See Table 217 for types, number ranges, and descriptions.
address	(Optional) NHRP mapping entry for specified protocol addresses.
interface	(Optional) NHRP mapping entry for the specified interface. See Table 217 for types, number ranges, and descriptions.
brief	(Optional) Displays a short output of the NHRP mapping.
detail	(Optional) Displays detailed information about NHRP mapping.
purge	(Optional) Displays NHRP purge information.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

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

Usage Guidelines

Table 217 lists the valid types, number ranges, and descriptions for the optional *interface* argument.

Note The valid types can vary according to the platform and interfaces on the platform.

Table 217 Valid Types, Number Ranges, and Interface Description

Valid Types	Number Ranges	Interface Descriptions
async	1	Async
atm	0 to 6	ATM

Table 217 Valid Types, Number Ranges, and Interface Description (continued)

Valid Types	Number Ranges	Interface Descriptions
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	FastEthernet 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 ipv6 nhrp** command:

```
Router# show ipv6 nhrp

2001:0db8:3c4d:0015::1a2f:3d2c/48  via
2001:0db8:3c4d:0015::1a2f:3d2c
Tunnel0 created 6d05h, never expire
```

Table 218 describes the significant fields shown in the display.

Table 218 show ipv6 nhrp Field Descriptions

Field	Description
2001:0db8:3c4d:0015::1a2f:3d2c/48	Target network.
2001:0db8:3c4d:0015::1a2f:3d2c	Next hop to reach the target network.
Tunnel0	Interface through which the target network is reached.
created 6d05h	Length of time since the entry was created (dayshours).
never expire	Indicates that static entries never expire.

The following is sample output from the **show ipv6 nhrp** command using the **brief** keyword:

```
Router# show ipv6 nhrp brief

2001:0db8:3c4d:0015:0000:0000:1a2f:3d2c/48
 via 2001:0db8:3c4d:0015:0000:0000:1a2f:3d2c
Interface: Tunnel0 Type: static
NBMA address: 10.11.11.99
```

Table 219 describes the significant fields shown in the display.

Table 219 show ipv6 nhrp brief Field Descriptions

Field	Description
2001:0db8:3c4d:0015:0000:0000:1a2f:3d2c/48	Target network.
via 2001:0db8:3c4d:0015:0000:0000:1a2f:3d2c	Next Hop to reach the target network.
Interface: Tunnel0	Interface through which the target network is reached.
Type: static	Type of tunnel. The types can be one of the following: • dynamic—NHRP mapping is obtained dynamically. The mapping entry is created using information from the NHRP resolution and registrations. • static—NHRP mapping is configured statically. Entries configured by the **ipv6 nhrp map** command are marked static. • incomplete—The NBMA address is not known for the target network.

Related Commands

Command	Description
ipv6 nhrp map	Statically configures the IPv6-to-NBMA address mapping of IP destinations connected to an NBMA network.

show ipv6 nhrp multicast

To display Next Hop Resolution Protocol (NHRP) multicast mapping information, use the **show ipv6 nhrp multicast** command in user EXEC or privileged EXEC mode.

show ipv6 nhrp multicast [*ipv6-address* | *interface*]

Syntax Description

ipv6-address	(Optional) The IPv6 address of the multicast mapping entry.
interface	(Optional) All multicast mapping entries of the NHRP network for the interface. See Table 220 for interface types, number ranges, and descriptions.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

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

Usage Guidelines

Table 220 lists the valid types, number ranges, and descriptions for the optional *interface* argument.

Note The valid types can vary according to the platform and interfaces on the platform.

Table 220 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	FastEthernet 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

Table 220 Valid Types, Number Ranges, and Interface Descriptions (continued)

Valid Types	Number Ranges	Interface Descriptions
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

Related Commands

Command	Description
ipv6 nhrp map	Statically configures the IPv6-to-NBMA address mapping of IPv6 destinations connected to an NBMA network.

show ipv6 nhrp nhs

To display Next Hop Resolution Protocol (NHRP) next hop server (NHS) information, use the **show ipv6 nhrp nhs** command in user EXEC or privileged EXEC mode.

show ipv6 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 220 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 cluster information. The range is from 0 to 10.
preempted	(Optional) Displays NHSs that come up and are preempted.
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
12.4(20)T	This command was introduced.
15.1(2)T	This command was modified. The **redundancy**, **cluster** *number*, **preempted**, **running**, and **waiting** keywords and argument were added.

Usage Guidelines

Table 220 lists the valid types, number ranges, and descriptions for the optional *interface-interface* argument.

Note The valid types can vary according to the platform and interfaces on the platform.

Table 221 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

Table 221 Valid Types, Number Ranges, and Interface Descriptions (continued)

Valid Types	Number Ranges	Interface Descriptions
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 ipv6 nhrp nhs** command:

```
Router# show ipv6 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 ipv6 nhrp nhs redundancy** command:

```
Router# show ipv6 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    5        2001::101   1         E          Running     RE        Running

No.  Interface  Cluster  Status  Max-Con  Total-NHS Responding Expecting Waiting Fallback
1    Tunnel0    5        Disable Not Set  1         0          1         0       0
```

Table 222 describes the significant field shown in the display.

Table 222 show ipv6 nhrp nhs Field Descriptions

Field	Description
Tunnel0	Interface through which the target network is reached.
priority	Priority value assigned to the NHS.
cluster	Group to which the NHS belong.
E=Expecting replies	NHSs that are active and expecting replies.
R=Responding	NHSs that are active and responding.
W=Waiting	NHSs that are preempted and are not in the active probe list.

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 ipv6 nhrp summary

To display Next Hop Resolution Protocol (NHRP) mapping summary information, use the **show ipv6 nhrp summary** command in user EXEC or privileged EXEC mode.

show ipv6 nhrp summary

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

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

Usage Guidelines

Use this command to monitor NHRP.

Examples

The following is sample output from the **show ipv6 nhrp summary** command:

```
Router# show ipv6 nhrp summary

IPV6 NHRP cache 1 entry, 256 bytes
    1 static  0 dynamic  0 incomplete
```

Table 222 describes the significant field shown in the display.

Table 223 show ipv6 nhrp summary Field Descriptions

Field Output	Description
static	NHRP mapping is configured statically. Entries configured by the **ipv6 nhrp map** command are marked static.
dynamic	NHRP mapping is obtained dynamically. The mapping entry is created using information from the NHRP resolution and registrations
incomplete	The nonbroadcast multiaccess (NBMA) address is not known for the target network.

Related Commands

Command	Description
ip nhrp map	Statically configures the IPv6-to-NBMA address mapping of IP destinations connected to an NBMA network.
show ipv6 nhrp	Displays NHRP mapping information.

show ipv6 nhrp traffic

To display Next Hop Resolution Protocol (NHRP) traffic statistics, use the **show ipv6 nhrp traffic** command in privileged EXEC mode.

show ipv6 nhrp traffic [*interface* **tunnel** *number*]

Syntax Description

interface	(Optional) Displays NHRP traffic information for a given interface.
tunnel *number*	(Optional) Specifies the tunnel interface number.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

Use this command to monitor NHRP traffic information.

Examples

The following example provides output for IPv6 NHRP traffic statistics:

```
Router# show ipv6 nhrp traffic

Tunnel0: Max-send limit:100Pkts/10Sec, Usage:0%
Sent: Total 8
1 Resolution Request 1 Resolution Reply 6 Registration Request
0 Registration Reply 0 Purge Request 0 Purge Reply
0 Error Indication 0 Traffic Indication
Rcvd: Total 5
1 Resolution Request 1 Resolution Reply 0 Registration Request
2 Registration Reply 0 Purge Request 0 Purge Reply
0 Error Indication 1 Traffic Indication
```

Table 222 describes the significant field shown in the display.

Table 224 show ipv6 nhrp traffic Field Descriptions

Field Output	Description
tunnel0:	Displays information about a specified tunnel; in thhis case, Tunnel0.
Max-send limit: 100Pkts/10Sec, Usage: 0%	The maximum number of packets allowed to be sent in a specified time, and the current usage.
Sent: Total 8	Number of packets sent.
1 Resolution Request 1 Resolution Reply 6 Registration Request 0 Registration Reply 0 Purge Request 0 Purge Reply	Description and breakdown of of the types of packets sent.

Table 224 show ipv6 nhrp traffic Field Descriptions (continued)

Field Output	Description
0 Error Indication 0 Traffic Indication	Number of errors in the sent packets.
Rcvd: Total 5	Number of packets received.
1 Resolution Request 1 Resolution Reply 0 Registration Request 2 Registration Reply 0 Purge Request 0 Purge Reply	Description and breakdown of the types of packets received.
0 Error Indication 1 Traffic Indication	Number of errors in the sent packets.

show ipv6 ospf

To display general information about Open Shortest Path First (OSPF) routing processes, use the **show ipv6 ospf** command in user EXEC or privileged EXEC mode.

show ipv6 ospf [*process-id*] [*area-id*] [**rate-limit**]

Syntax Description

process-id	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when the OSPF routing process is enabled.
area-id	(Optional) Area ID. This argument displays information about a specified area only.
rate-limit	(Optional) Rate-limited link-state advertisements (LSAs). This keyword displays LSAs that are currently being rate limited, together with the remaining time to the next generation.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.3(4)T	Command output is changed when authentication is enabled.
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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(9)T	Command output was updated to display OSPF for IPv6 encryption information.
12.4(15)XF	Command output was modified to include VMI PPPoE process-level values.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SRC	The **rate-limit** keyword was added. Command output was modified to include the configuration values for SPF and LSA throttling timers.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.0(1)M	This command was integrated into Cisco IOS Release 12.5(1)M.
15.1(2)T	This command was modified. Support for IPv6 was added to Cisco IOS Release 15.1(2)T.

Examples

show ipv6 ospf Output Example

The following is sample output from the **show ipv6 ospf** command:

```
Router# show ipv6 ospf

Routing Process "ospfv3 1" with ID 10.10.10.1
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
    Area BACKBONE(0)
        Number of interfaces in this area is 1
        MD5 Authentication, SPI 1000
        SPF algorithm executed 2 times
        Number of LSA 5. Checksum Sum 0x02A005
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

Table 225 describes the significant fields shown in the display.

Table 225 show ipv6 ospf Field Descriptions

Field	Description
Routing process “ospfv3 1” with ID 10.10.10.1	Process ID and OSPF router ID.
LSA group pacing timer	Configured LSA group pacing timer (in seconds).
Interface flood pacing timer	Configured LSA flood pacing timer (in milliseconds).
Retransmission pacing timer	Configured LSA retransmission pacing timer (in milliseconds).
Number of areas	Number of areas in router, area addresses, and so on.

show ipv6 ospf With Area Encryption Example

The following sample output shows the **show ipv6 ospf** command with area encryption information:

```
Router# show ipv6 ospf

Routing Process "ospfv3 1" with ID 10.0.0.1
It is an area border router
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msecs
Retransmission pacing timer 66 msecs
Number of external LSA 0. Checksum Sum 0x000000
Number of areas in this router is 2. 2 normal 0 stub 0 nssa
Reference bandwidth unit is 100 mbps
    Area BACKBONE(0)
        Number of interfaces in this area is 2
        SPF algorithm executed 3 times
        Number of LSA 31. Checksum Sum 0x107493
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 20
        Flood list length 0
```

```
    Area 1
        Number of interfaces in this area is 2
        NULL Encryption SHA-1 Auth, SPI 1001
        SPF algorithm executed 7 times
        Number of LSA 20. Checksum Sum 0x095E6A
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

Table 226 describes the significant fields shown in the display.

Table 226 show ipv6 ospf with Area Encryption Information Field Descriptions

Field	Description
Area 1	Subsequent fields describe area 1.
NULL Encryption SHA-1 Auth, SPI 1001	Displays the encryption algorithm (in this case, null, meaning no encryption algorithm is used), the authentication algorithm (SHA-1), and the security policy index (SPI) value (1001).

The following example displays the configuration values for SPF and LSA throttling timers:

```
Router# show ipv6 ospf

 Routing Process "ospfv3 1" with ID 10.9.4.1
 Event-log enabled, Maximum number of events: 1000, Mode: cyclic
 It is an autonomous system boundary router
 Redistributing External Routes from,
    ospf 2
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Minimum LSA interval 5 secs
 Minimum LSA arrival 1000 msecs
```

Table 227 describes the significant fields shown in the display.

Table 227 show ipv6 ospf with SPF and LSA Throttling Timer Field Descriptions

Field	Description
Initial SPF schedule delay	Delay time of SPF calculations.
Minimum hold time between two consecutive SPFs	Minimum hold time between consecutive SPF calculations.
Maximum wait time between two consecutive SPFs 10000 msecs	Maximum hold time between consecutive SPF calculations.
Minimum LSA interval 5 secs	Minimum time interval (in seconds) between link-state advertisements.
Minimum LSA arrival 1000 msecs	Maximum arrival time (in milliseconds) of link-state advertisements.

The following example shows information about LSAs that are currently being rate limited:

```
Router# show ipv6 ospf rate-limit

List of LSAs that are in rate limit Queue
```

```
LSAID: 0.0.0.0 Type: 0x2001 Adv Rtr: 10.55.55.55 Due in: 00:00:00.500
LSAID: 0.0.0.0 Type: 0x2009 Adv Rtr: 10.55.55.55 Due in: 00:00:00.500
```

Table 228 describes the significant fields shown in the display.

Table 228 show ipv6 ospf rate-limit Field Descriptions

Field	Description
LSAID	Link-state ID of the LSA.
Type	Description of the LSA.
Adv Rtr	ID of the advertising router.
Due in:	Remaining time until the generation of the next event.

show ipv6 ospf border-routers

To display the internal Open Shortest Path First (OSPF) routing table entries to an Area Border Router (ABR) and Autonomous System Boundary Router (ASBR), use the **show ipv6 ospf border-routers** command in user EXEC or privileged EXEC mode.

show ip ospf [*process-id*] **border-routers**

Syntax Description

process-id	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when the OSPF routing process is enabled.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)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.

Examples

The following is sample output from the **show ipv6 ospf border-routers** command:

```
Router# show ipv6 ospf border-routers

OSPFv3 Process 1 internal Routing Table

Codes: i - Intra-area route, I - Inter-area route

i 172.16.4.4 [2] via FE80::205:5FFF:FED3:5808, FastEthernet0/0, ABR, Area 1, SPF 13
i 172.16.4.4 [1] via FE80::205:5FFF:FED3:5406, POS4/0, ABR, Area 0, SPF 8
i 172.16.3.3 [1] via FE80::205:5FFF:FED3:5808, FastEthernet0/0, ASBR, Area 1, SPF 3
```

Table 229 describes the significant fields shown in the display.

Table 229 show ipv6 ospf border-routers Field Descriptions

Field	Description
i - Intra-area route, I - Inter-area route	The type of this route.
172.16.4.4, 172.16.3.3	Router ID of the destination router.
[2], [1]	Metric used to reach the destination router.

Table 229 show ipv6 ospf border-routers Field Descriptions (continued)

Field	Description
FE80::205:5FFF:FED3:5808, FE80::205:5FFF:FED3:5406, FE80::205:5FFF:FED3:5808	Link-local routers.
FastEthernet0/0, POS4/0	The interface on which the IPv6 OSPF protocol is configured.
ABR	Area border router.
ASBR	Autonomous system boundary router.
Area 0, Area 1	The area ID of the area from which this route is learned.
SPF 13, SPF 8, SPF 3	The internal number of the shortest path first (SPF) calculation that installs this route.

show ipv6 ospf database

To display lists of information related to the Open Shortest Path First (OSPF) database for a specific router, use the **show ipv6 ospf database** command in user EXEC or privileged EXEC mode. The various forms of this command deliver information about different OSPF link-state advertisements (LSAs).

show ipv6 ospf [*process-id* [*area-id*]] **database** [**adv-router** *router-id* | **self-originate**] [**internal**]

show ipv6 ospf [*process-id* [*area-id*]] **database** [**database-summary**]

show ipv6 ospf [*process-id* [*area-id*]] **database** [**external** [*ipv6-prefix*] [*link-state-id*]] | [**adv-router** *router-id* | **self-originate**] [**internal**]

show ipv6 ospf [*process-id* [*area-id*]] **database** [**grace**]

show ipv6 ospf [*process-id* [*area-id*]] **database** [**inter-area prefix** [*ipv6-prefix*] [*link-state-id*]] | [**adv-router** *router-id* | **self-originate**] [**internal**]

show ipv6 ospf [*process-id* [*area-id*]] **database** [**inter-area router** [*destination-router-id*] [*link-state-id*]] | [**adv-router** *router-id* | **self-originate**] [**internal**]

show ipv6 ospf [*process-id* [*area-id*]] **database** [**link** [**interface** *interface-name*] [*link-state-id*]] [**adv-router** *router-id* | **self-originate**] [**internal**]

show ipv6 ospf [*process-id* [*area-id*]] **database** [**network** [*link-state-id*]] [**adv-router** *router-id* | **self-originate**] [**internal**]

show ipv6 ospf [*process-id* [*area-id*]] **database** [**nssa-external** [*ipv6-prefix*] [*link-state-id*]] [**adv-router** *router-id* | **self-originate**] [**internal**]

show ipv6 ospf [*process-id* [*area-id*]] **database** [**prefix** [**ref-lsa** {**router** | **network**}] [*link-state-id*]] [**adv-router** *router-id* | **self-originate**] [**internal**]

show ipv6 ospf [*process-id* [*area-id*]] **database** [**router** [*link-state-id*]] [**adv-router** *router-id* | **self-originate**] [**internal**]

show ipv6 ospf [*process-id* [*area-id*]] **database** [[**router** | **network** | [**external** *ipv6-prefix* | **nssa-external** *ipv6-prefix* | **inter-area** {**prefix** *ipv6-prefix* | **router**}] | **link** | **prefix**] | **database-summary**] [**adv-router** *router-id* | **self-originate**] [**internal**]

show ipv6 ospf [*process-id* [*area-id*]] **database** [**unknown** [{**area** | **as** | **link**} [*link-state-id*]]] [**adv-router** *router-id* | **self-originate**] [**internal**]

Syntax Description

process-id	(Optional) Displays information only about a specified process.
area-id	(Optional) Displays information only about a specified area. The *area-id* argument can only be used if the *process-id* argument is specified.
adv-router *router-id*	(Optional) Displays all the LSAs of the advertising router. This argument must be in the form documented in RFC 2740 where the address is specified in hexadecimal using 16-bit values between colons.
self-originate	(Optional) Displays only self-originated LSAs (from the local router).
internal	(Optional) Internal LSA information.
database-summary	(Optional) Displays how many of each type of LSAs exist for each area in the database, and the total.
external	(Optional) Displays information only about the external LSAs.
ipv6-prefix	(Optional) Link-local IPv6 address of the neighbor. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
link-state-id	(Optional) An integer used to differentiate LSAs. In network and link LSAs, the link-state ID matches the interface index.
inter-area prefix	(Optional) Displays information only about LSAs based on inter-area prefix LSAs.
inter-area router	(Optional) Displays information only about LSAs based on inter-area router LSAs.
destination-router-id	(Optional) The specified destination router ID.
link	(Optional) Displays information about the link LSAs.
interface	(Optional) Displays information about the LSAs filtered by interface context.
interface-name	(Optional) Specifies the LSA interface.
network	(Optional) Displays information only about the network LSAs.
nssa-external	(Optional) Displays information only about the not so stubby area (NSSA) external LSAs.
prefix	(Optional) Displays information on the intra-area-prefix LSAs.
ref-lsa {**router** | **network**}	(Optional) Further filters the prefix LSA type.
router	(Optional) Displays information only about the router LSAs.
unknown	(Optional) Displays all LSAs with unknown types.
area	(Optional) Filters unknown area LSAs.
as	(Optional) Filters unknown autonomous system (AS) LSAs.
link	(Optional) When following the **unknown** keyword, the **link** keyword filters link-scope LSAs.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)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	The **grace** keyword was added to show information about OSPFv3 graceful restart.

Usage Guidelines

The **adv-router** keyword requires a router ID. The **self-originate** keyword displays only those LSAs that originated from the local router. Both of these keywords can be appended to all other keywords used with the **show ipv6 ospf** database command to provide more detailed information.

Examples

The following is sample output from the **show ipv6 ospf database** command when no arguments or keywords are used:

```
Router# show ipv6 ospf database

            OSPFv3 Router with ID (172.16.4.4) (Process ID 1)

                Router Link States (Area 0)

ADV Router         Age         Seq#        Fragment ID   Link count  Bits
172.16.4.4         239         0x80000003  0             1           B
172.16.6.6         239         0x80000003  0             1           B

            Inter Area Prefix Link States (Area 0)

ADV Router         Age         Seq#        Prefix
172.16.4.4         249         0x80000001  FEC0:3344::/32
172.16.4.4         219         0x80000001  FEC0:3366::/32
172.16.6.6         247         0x80000001  FEC0:3366::/32
172.16.6.6         193         0x80000001  FEC0:3344::/32
172.16.6.6         82          0x80000001  FEC0::/32

            Inter Area Router Link States (Area 0)

ADV Router         Age         Seq#        Link ID    Dest RtrID
172.16.4.4         219         0x80000001  50529027   172.16.3.3
172.16.6.6         193         0x80000001  50529027   172.16.3.3

            Link (Type-8) Link States (Area 0)

ADV Router         Age         Seq#        Link ID    Interface
172.16.4.4         242         0x80000002  14         PO4/0
172.16.6.6         252         0x80000002  14         PO4/0

            Intra Area Prefix Link States (Area 0)

ADV Router         Age         Seq#        Link ID    Ref-lstype  Ref-LSID
172.16.4.4         242         0x80000002  0          0x2001      0
172.16.6.6         252         0x80000002  0          0x2001      0
```

Table 230 describes the significant fields shown in the display.

Table 230 show ipv6 ospf database Field Descriptions

Field	Description
ADV Router	Advertising router ID.
Age	Link-state age.
Seq#	Link-state sequence number (detects old or duplicate LSAs).
Link ID	Interface ID number.
Ref-lstype	Referenced link-state type.
Ref-LSID	Referenced link-state ID.

The following is sample output from the **show ipv6 ospf database** command with the **router self-originate** keywords:

```
Router# show ipv6 ospf database router self-originate

            OSPFv3 Router with ID (172.16.6.6) (Process ID 1)

            Router Link States (Area 0)

  LS age: 383
  Options: (V6-Bit E-Bit R-bit DC-Bit)
  LS Type: Router Links
  Link State ID: 0
  Advertising Router: 172.16.6.6
  LS Seq Number: 80000003
  Checksum: 0x7543
  Length: 40
  Area Border Router
  Number of Links: 1

    Link connected to: another Router (point-to-point)
      Link Metric: 1
      Local Interface ID: 14
      Neighbor Interface ID: 14
      Neighbor Router ID: 172.16.4.4
```

The following is sample output from the **show ipv6 ospf database** command with the **network** keyword:

```
Router# show ipv6 ospf database network

            OSPFv3 Router with ID (172.16.6.6) (Process ID 1)

            Net Link States (Area 1)

  LS age: 419
  Options: (V6-Bit E-Bit R-bit DC-Bit)
  LS Type: Network Links
  Link State ID: 3 (Interface ID of Designated Router)
  Advertising Router: 172.16.6.6
  LS Seq Number: 80000001
  Checksum: 0x8148
  Length: 32
        Attached Router: 172.16.6.6
        Attached Router: 172.16.3.3
```

The following is sample output from the **show ipv6 ospf database** command with the **link self-originate** keywords:

```
Router# show ipv6 ospf database link self-originate

            OSPFv3 Router with ID (172.16.6.6) (Process ID 1)

            Link (Type-8) Link States (Area 0)

  LS age: 505
  Options: (V6-Bit E-Bit R-bit DC-Bit)
  LS Type: Link-LSA (Interface: POS4/0)
  Link State ID: 14 (Interface ID)
  Advertising Router: 172.16.6.6
  LS Seq Number: 80000002
  Checksum: 0xABF6
  Length: 60
  Router Priority: 1
  Link Local Address: FE80::205:5FFF:FED3:6408
  Number of Prefixes: 2
  Prefix Address: FEC0:4466::
  Prefix Length: 32, Options: None
  Prefix Address: FEC0:4466::
  Prefix Length: 32, Options: None
```

The following is sample output from the **show ipv6 ospf database** command with the **prefix self-originate** keywords:

```
Router# show ipv6 ospf database prefix self-originate

            OSPFv3 Router with ID (172.16.6.6) (Process ID 1)

            Intra Area Prefix Link States (Area 0)

  Routing Bit Set on this LSA
  LS age: 552
  LS Type: Intra-Area-Prefix-LSA
  Link State ID: 0
  Advertising Router: 172.16.6.6
  LS Seq Number: 80000002
  Checksum: 0xA910
  Length: 48
  Referenced LSA Type: 2001
  Referenced Link State ID: 0
  Referenced Advertising Router: 172.16.6.6
  Number of Prefixes: 2
  Prefix Address: FEC0:4466::
  Prefix Length: 32, Options: None, Metric: 1
  Prefix Address: FEC0:4466::
  Prefix Length: 32, Options: None, Metric: 1
```

The following is sample output from the **show ipv6 ospf database** command with the **inter-area prefix self-originate** keywords:

```
Router# show ipv6 ospf database inter-area prefix self-originate

            OSPFv3 Router with ID (172.16.6.6) (Process ID 1)

            Inter Area Prefix Link States (Area 0)

  LS age: 587
  LS Type: Inter Area Prefix Links
  Link State ID: 0
  Advertising Router: 172.16.6.6
```

```
  LS Seq Number: 80000001
  Checksum: 0x1395
  Length: 32
  Metric: 1
  Prefix Address: FEC0:3366::
  Prefix Length: 32, Options: None

  LS age: 532
  LS Type: Inter Area Prefix Links
  Link State ID: 1
  Advertising Router: 172.16.6.6
  LS Seq Number: 80000001
  Checksum: 0x3197
  Length: 32
  Metric: 2
  Prefix Address: FEC0:3344::
  Prefix Length: 32, Options: None

  LS age: 422
  LS Type: Inter Area Prefix Links
  Link State ID: 2
  Advertising Router: 172.16.6.6
  LS Seq Number: 80000001
  Checksum: 0xCB74
  Length: 32
  Metric: 1
  Prefix Address: FEC0::
  Prefix Length: 32, Options: None
```

The following is sample output from the **show ipv6 ospf database** command with the **inter-area router self-originate** keywords:

```
Router# show ipv6 ospf database inter-area router self-originate

            OSPFv3 Router with ID (172.16.6.6) (Process ID 1)

            Inter Area Router Link States (Area 0)

  LS age: 578
  Options: (V6-Bit E-Bit R-bit DC-Bit)
  LS Type: Inter Area Router Links
  Link State ID: 50529027
  Advertising Router: 172.16.6.6
  LS Seq Number: 80000001
  Checksum: 0x369F
  Length: 32
  Metric: 1
  Destination Router ID: 172.16.3.3
```

The following is sample output from the **show ipv6 ospf database** command with the **external** keyword:

```
Router# show ipv6 ospf database external

            OSPFv3 Router with ID (172.16.6.6) (Process ID 1)

            Type-5 AS External Link States

  Routing Bit Set on this LSA
  LS age: 654
  LS Type: AS External Link
  Link State ID: 0
  Advertising Router: 172.16.3.3
  LS Seq Number: 80000001
  Checksum: 0x218D
```

```
  Length: 32
  Prefix Address: FEC0:3333::
  Prefix Length: 32, Options: None
  Metric Type: 2 (Larger than any link state path)
  Metric: 20
```

The following is sample output from the **show ipv6 ospf database** command for a graceful-restart-capable router:

```
Router# show ipv6 ospf 1 database

            OSPFv3 Router with ID (10.2.2.2) (Process ID 1)

            Router Link States (Area 0)
ADV Router      Age         Seq#             Fragment ID  Link count  Bits
10.1.1.1         1949       0x8000000e          0            1        None
10.2.2.2         2007       0x80000011          0            1        None

            Link (Type-8) Link States (Area 0)
ADV Router      Age         Seq#              Link ID    Interface
10.1.1.1         180         0x80000006         1         PO0/2/0/0
10.2.2.2        2007         0x80000006         1         PO0/2/0/0

            Intra Area Prefix Link States (Area 0)
ADV Router      Age         Seq#              Link ID    Ref-lstype  Ref-LSID
10.1.1.1        180         0x80000006          0        0x2001          0
10.2.2.2        2007        0x80000006          0        0x2001          0

            Grace (Type-11) Link States (Area 0)
ADV Router      Age         Seq#                Link ID    Interface
10.2.2.2        2007        0x80000005            1        PO0/2/0/0
```

The following is sample outpet from the **show ipv6 ospf database** command with the **grace** keyword:

```
Router# show ipv6 ospf database grace

OSPFv3 Router with ID (10.3.33.3) (Process ID 1)

Grace (Type-11) Link States (Area 0)

  LS age: 2
  LS Type: Grace Links (Interface: Ethernet0/0)
  Link State ID: 3 (Interface ID)
  Advertising Router: 10.2.2.2
  LS Seq Number: 80000001
  Checksum: 0xE3DD
  Length: 36
  Grace Period : 120
        Graceful Restart Reason : Software reload/upgrade
```

Table 231 describes the significant fields shown in the display.

Table 231 show ipv6 ospf database Field Descriptions

Field	Description
Grace (Type-11)	Type 11 indicates that this router is graceful-restart capable.
LS Type: Grace Links (Interfece: Ethernet 0/0)	The link state type and interface used.

Table 231 show ipv6 ospf database Field Descriptions

Field	Description
Grace Period : 120	The graceful-restart interval, in seconds.
Graceful Restart Reason: Software reload/upgrade	The reason graceful restart was activated .

Related Commands

Command	Description
show ipv6 ospf	Displays general information about OSPFv3 routing processes.
show ipv6 ospf graceful-restart	Displays OSPFv3 graceful restart information.
show ipv6 ospf interface	Displays OSPFv3-related interface information.

show ipv6 ospf event

To display detailed information about IPv6 Open Shortest Path First (OSPF) events, use the **show ipv6 ospf event** command in privileged EXEC mode.

show ipv6 ospf [*process-id*] **event** [**generic** | **interface** | **lsa** | **neighbor** | **reverse** | **rib** | **spf**]

Syntax Description

process-id	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when the OSPF routing process is enabled.
generic	(Optional) Generic information regarding OSPF for IPv6 events.
interface	(Optional) Interface state change events, including old and new states.
lsa	(Optional) LSA arrival and LSA generation events.
neighbor	(Optional) Neighbor state change events, including old and new states.
reverse	(Optional) Keyword to allow the display of events in reverse–from the latest to the oldest or from oldest to the latest.
rib	(Optional) Routing Information Base (RIB) update, delete, and redistribution events.
spf	(Optional) Scheduling and SPF run events.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

An OSPF event log is kept for every OSPF instance. If you enter no keywords with the **show ipv6 ospf event** command, all information in the OSPF event log is displayed. Use the keywords to filter specific information.

Examples

The following example shows scheduling and SPF run events, LSA arrival and LSA generation events, in order from the oldest events to the latest generated events:

```
Router# show ipv6 ospf event spf lsa reverse

OSPFv3 Router with ID (10.0.0.1) (Process ID 1)

1 *Sep 29 11:59:18.367: Rcv Changed Type-0x2009 LSA, LSID 10.0.0.0, Adv-Rtr 192.168.0.1,
Seq# 80007699, Age 3600
```

```
3 *Sep 29 11:59:18.367: Schedule SPF, Area 0, Change in LSID 10.0.0.0, LSA type P
4 *Sep 29 11:59:18.367: Rcv Changed Type-0x2001 LSA, LSID 10.0.0.0, Adv-Rtr 192.168.0.1,
Seq# 80007699, Age 2
5 *Sep 29 11:59:18.367: Schedule SPF, Area 0, Change in LSID 10.0.0.0, LSA type R
6 *Sep 29 11:59:18.367: Rcv Changed Type-0x2002 LSA, LSID 10.1.0.1, Adv-Rtr 192.168.0.1,
Seq# 80007699, Age 3600
8 *Sep 29 11:59:18.367: Schedule SPF, Area 0, Change in LSID 10.1.0.1, LSA type N
9 *Sep 29 11:59:18.367: Rcv Changed Type-0x2001 LSA, LSID 10.0.0.0, Adv-Rtr 1.1.1.1, Seq#
80007699, Age 2
10 *Sep 29 11:59:18.367: Schedule SPF, Area 0, Change in LSID 10.0.0.0, LSA type R
11 *Sep 29 11:59:18.867: Starting SPF
12 *Sep 29 11:59:18.867: Starting Intra-Area SPF in Area 0
16 *Sep 29 11:59:18.867: Starting Inter-Area SPF in area 0
17 *Sep 29 11:59:18.867: Starting External processing
18 *Sep 29 11:59:18.867: Starting External processing in area 0
19 *Sep 29 11:59:18.867: Starting External processing in area 1
20 *Sep 29 11:59:18.867: End of SPF
21 *Sep 29 11:59:19.367: Generate Changed Type-0x2003 LSA, LSID 10.0.0.4, Seq# 80000002,
Age 3600, Area 1, Prefix 3000:11:22::/64
23 *Sep 29 11:59:20.367: Rcv Changed Type-0x2009 LSA, LSID 10.0.0.0, Adv-Rtr 192.168.0.1,
Seq# 8000769A, Age 2
24 *Sep 29 11:59:20.367: Schedule SPF, Area 0, Change in LSID 10.0.0.0, LSA type P
25 *Sep 29 11:59:20.367: Rcv Changed Type-0x2001 LSA, LSID 10.0.0.0, Adv-Rtr 192.168.0.1,
Seq# 8000769A, Age 2
26 *Sep 29 11:59:20.367: Schedule SPF, Area 0, Change in LSID 10.0.0.0, LSA type R
27 *Sep 29 11:59:20.367: Rcv Changed Type-0x2002 LSA, LSID 10.1.0.1, Adv-Rtr 192.168.0.1,
Seq# 8000769A, Age 2
28 *Sep 29 11:59:20.367: Schedule SPF, Area 0, Change in LSID 10.1.0.1, LSA type N
29 *Sep 29 11:59:20.367: Rcv Changed Type-0x2001 LSA, LSID 10.0.0.0, Adv-Rtr 1.1.1.1, Seq#
8000769A, Age 2
30 *Sep 29 11:59:20.367: Schedule SPF, Area 0, Change in LSID 10.0.0.0, LSA type R
31 *Sep 29 11:59:20.867: Starting SPF
32 *Sep 29 11:59:20.867: Starting Intra-Area SPF in Area 0
36 *Sep 29 11:59:20.867: Starting Inter-Area SPF in area 0
37 *Sep 29 11:59:20.867: Starting External processing
38 *Sep 29 11:59:20.867: Starting External processing in area 0
39 *Sep 29 11:59:20.867: Starting External processing in area 1
40 *Sep 29 11:59:20.867: End of SPF
```

Table 232 describes the significant fields shown in the display.

Table 232 show ip ospf Field Descriptions

Field	Description
OSPFv3 Router with ID (10.0.0.1) (Process ID 1)	Process ID and OSPF router ID.
Rcv Changed Type-0x2009 LSA	Description of newly arrived LSA.
LSID	Link-state ID of the LSA.
Adv-Rtr	ID of the advertising router.
Seq#	Link state sequence number (detects old or duplicate link state advertisements).
Age	Link state age (in seconds).
Schedule SPF	Enables SPF to run.
Area	OSPF area ID.
Change in LSID	Changed link-state ID of the LSA.
LSA type	LSA type.

show ipv6 ospf flood-list

To display a list of Open Shortest Path First (OSPF) link-state advertisements (LSAs) waiting to be flooded over an interface, use the **show ipv6 ospf flood-list** command in user EXEC or privileged EXEC mode.

show ipv6 ospf [*process-id*] [*area-id*] **flood-list** *interface-type interface-number*

Syntax Description

process-id	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when the OSPF routing process is enabled.
area-id	(Optional) Displays information only about a specified area.
interface-type	Interface type over which the LSAs will be flooded.
interface-number	Interface number over which the LSAs will be flooded.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)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.

Usage Guidelines

Use this command to display OSPF packet pacing.

Examples

The following is sample output from the **show ipv6 ospf flood-list** command:

```
Router# show ipv6 ospf flood-list

OSPFv3 Router with ID (172.16.6.6) (Process ID 1)

 Interface POS4/0, Queue length 1
 Link state retransmission due in 14 msec

 Type    LS ID           ADV RTR         Seq NO      Age    Checksum
 0x2001  0               172.16.6.6      0x80000031  0      0x1971

 Interface FastEthernet0/0, Queue length 0

 Interface ATM3/0, Queue length 0
```

Table 233 describes the significant fields shown in the display.

Table 233 show ipv6 ospf flood-list Field Descriptions

Field	Description
OSPFv3 Router with ID (172.16.6.6) (Process ID 1)	Identification of the router for which information is displayed.
Interface POS4/0	Interface for which information is displayed.
Queue length	Number of LSAs waiting to be flooded.
Link state retransmission due in	Length of time before next link-state transmission.
Type	Type of LSA.
LS ID	Link-state ID of the LSA.
ADV RTR	IP address of advertising router.
Seq NO	Sequence number of LSA.
Age	Age of LSA (in seconds).
Checksum	Checksum of LSA.

show ipv6 ospf graceful-restart

To display Open Shortest Path First for IPv6 (OSPFv3) graceful restart information, use the **show ipv6 ospf graceful-restart** command in privileged EXEC mode.

show ipv6 ospf graceful-restart

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 12.5(1)M.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

Use the **show ipv6 ospf graceful-restart** command to discover information about the OSPFv3 graceful restart feature.

Examples

The following example displays OSPFv3 graceful restart information:

```
Router# show ipv6 ospf graceful-restart

Routing Process "ospf 1"
 Graceful Restart enabled
    restart-interval limit: 120 sec, last restart 00:00:15 ago (took 36 secs)
  Graceful Restart helper support enabled
  Router status : Active
  Router is running in SSO mode
  OSPF restart state : NO_RESTART
  Router ID 10.1.1.1, checkpoint Router ID 10.0.0.0
```

Table 230 describes the significant fields shown in the display.

Table 234 show ipv6 ospf graceful-restart Field Descriptions

Field	Description
Routing Process “ospf 1”	The OSPFv3 routing process ID.
Graceful Restart enabled	The graceful restart feature is enabled on this router.

Table 234 show ipv6 ospf graceful-restart Field Descriptions (continued)

Field	Description
restart-interval limit: 120 sec	The restart-interval limit.
last restart 00:00:15 ago (took 36 secs)	How long ago the last graceful restart occurred, and how long it took to occur.
Graceful Restart helper support enabled	Graceful restart helper mode is enabled. Because graceful restart mode is also enabled on this router, you can identify this router as being graceful-restart capable. A router that is graceful-restart-aware cannot be configured in graceful-restart mode.
Router status : Active	This router is in active, as opposed to standby, mode.
Router is running in SSO mode	The router is in stateful switchover mode.
OSPF restart state : NO_RESTART	The current OSPFv3 restart state.
Router ID 10.1.1.1, checkpoint Router ID 10.0.0.0	The IPv6 addresses of the current router and the checkpoint router.

Related Commands

Command	Description
show ipv6 ospf interface	Displays OSPFv3-related interface information.

show ipv6 ospf interface

To display Open Shortest Path First (OSPF)-related interface information, use the **show ipv6 ospf interface** command in user EXEC or privileged mode.

show ipv6 ospf [*process-id*] [*area-id*] **interface** [*type number*] [**brief**]

Syntax Description

process-id	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when the OSPF routing process is enabled.
area-id	(Optional) Displays information about a specified area only.
type number	(Optional) Interface type and number.
brief	(Optional) Displays brief overview information for OSPF interfaces, states, addresses and masks, and areas on the router.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.3(4)T	Command output is changed when authentication is enabled.
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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(9)T	Command output is changed when encryption is enabled.
12.2(33)SRB	The **brief** keyword was added.
12.4(15)XF	Output displays were modified so that VMI PPPoE interface-based local state values are displayed in the command output when a VMI interface is specified.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	Command output was updated to display graceful restart information.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.

Examples

show ipv6 ospf interface Standard Output Example

The following is sample output from the **show ipv6 ospf interface** command:

```
Router# show ipv6 ospf interface
```

```
ATM3/0 is up, line protocol is up
  Link Local Address 2001:0DB1:205:5FFF:FED3:5808, Interface ID 13
  Area 1, Process ID 1, Instance ID 0, Router ID 172.16.3.3
  Network Type POINT_TO_POINT, Cost: 1
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
  Index 1/2/2, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 12, maximum is 12
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 172.16.4.4
  Suppress hello for 0 neighbor(s)
FastEthernet0/0 is up, line protocol is up
  Link Local Address 2001:0DB1:205:5FFF:FED3:5808, Interface ID 3
  Area 1, Process ID 1, Instance ID 0, Router ID 172.16.3.3
  Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 172.16.6.6, local address 2001:0DB1:205:5FFF:FED3:6408
  Backup Designated router (ID) 172.16.3.3, local address 2001:0DB1:205:5FFF:FED3:5808
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 12, maximum is 12
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 172.16.6.6  (Designated Router)
  Suppress hello for 0 neighbor(s)
```

Table 235 describes the significant fields shown in the display.

Table 235 show ipv6 ospf interface Field Descriptions

Field	Description
ATM3/0	Status of the physical link and operational status of protocol.
Link Local Address	Interface IPv6 address.
Area 1, Process ID 1, Instance ID 0, Router ID 172.16.3.3	The area ID, process ID, instance ID, and router ID of the area from which this route is learned.
Network Type POINT_TO_POINT, Cost: 1	Network type and link-state cost.
Transmit Delay	Transmit delay, interface state, and router priority.
Designated Router	Designated router ID and respective interface IP address.
Backup Designated router	Backup designated router ID and respective interface IP address.
Timer intervals configured	Configuration of timer intervals.
Hello	Number of seconds until the next hello packet is sent out this interface.
Neighbor Count	Count of network neighbors and list of adjacent neighbors.

Cisco IOS Release 12.2(33)SRB Example

The following is sample output of the **show ipv6 ospf interface** command when the **brief** keyword is entered.

```
Router# show ipv6 ospf interface brief

Interface    PID   Area            Intf ID    Cost  State Nbrs F/C
VL0          6     0               21         65535 DOWN  0/0
Se3/0        6     0               14         64    P2P   0/0
Lo1          6     0               20         1     LOOP  0/0
Se2/0        6     6               10         62    P2P   0/0
Tu0          1000  0               19         11111 DOWN  0/0
```

OSPF with Authentication on the Interface Example

The following is sample output from the **show ipv6 ospf interface** command with authentication enabled on the interface:

```
Router# show ipv6 ospf interface

Ethernet0/0 is up, line protocol is up
  Link Local Address 2001:0DB1:A8BB:CCFF:FE00:6E00, Interface ID 2
  Area 0, Process ID 1, Instance ID 0, Router ID 10.10.10.1
  Network Type BROADCAST, Cost:10
  MD5 Authentication SPI 500, secure socket state UP (errors:0)
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 10.11.11.1, local address 2001:0DB1:A8BB:CCFF:FE00:6F00
  Backup Designated router (ID) 10.10.10.1, local address
2001:0DB1:A8BB:CCFF:FE00:6E00
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:01
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.11.11.1  (Designated Router)
  Suppress hello for 0 neighbor(s)
```

OSPF with Null Authentication Example

The following is sample output from the **show ipv6 ospf interface** command with null authentication configured on the interface:

```
Router# show ipv6 ospf interface

Ethernet0/0 is up, line protocol is up
  Link Local Address 2001:0DB1:A8BB:CCFF:FE00:6E00, Interface ID 2
  Area 0, Process ID 1, Instance ID 0, Router ID 10.10.10.1
  Network Type BROADCAST, Cost:10
  Authentication NULL
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 10.11.11.1, local address 2001:0DB1:A8BB:CCFF:FE00:6F00
  Backup Designated router (ID) 10.10.10.1, local address
2001:0DB1:A8BB:CCFF:FE00:6E00
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:03
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.11.11.1  (Designated Router)
```

```
  Suppress hello for 0 neighbor(s)
```

OSPF with Authentication for the Area Example

The following is sample output from the **show ipv6 ospf interface** command with authentication configured for the area:

```
Router# show ipv6 ospf interface

Ethernet0/0 is up, line protocol is up
  Link Local Address 2001:0DB1:A8BB:CCFF:FE00:6E00, Interface ID 2
  Area 0, Process ID 1, Instance ID 0, Router ID 10.10.10.1
  Network Type BROADCAST, Cost:10
  MD5 Authentication (Area) SPI 1000, secure socket state UP (errors:0)
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 10.11.11.1, local address 2001:0DB1:A8BB:CCFF:FE00:6F00
  Backup Designated router (ID) 10.10.10.1, local address
FE80::A8BB:CCFF:FE00:6E00
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:03
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.11.11.1  (Designated Router)
  Suppress hello for 0 neighbor(s)
```

OSPF with Dynamic Cost Example

The following display shows sample output from the **show ipv6 ospf interface** command when the OSPF cost dynamic is configured.

```
Router1# show ipv6 ospf interface serial 2/0

Serial2/0 is up, line protocol is up
   Link Local Address 2001:0DB1:A8BB:CCFF:FE00:100, Interface ID 10
   Area 1, Process ID 1, Instance ID 0, Router ID 172.1.1.1
   Network Type POINT_TO_MULTIPOINT, Cost: 64 (dynamic), Cost Hysteresis: 200
   Cost Weights: Throughput 100, Resources 20, Latency 80, L2-factor 100
   Transmit Delay is 1 sec, State POINT_TO_MULTIPOINT,
   Timer intervals configured, Hello 30, Dead 120, Wait 120, Retransmit 5
     Hello due in 00:00:19
   Index 1/2/3, flood queue length 0
   Next 0x0(0)/0x0(0)/0x0(0)
   Last flood scan length is 0, maximum is 0
   Last flood scan time is 0 msec, maximum is 0 msec
   Neighbor Count is 0, Adjacent neighbor count is 0
   Suppress hello for 0 neighbor(s)
```

OSPF Graceful Restart Example

The following display shows sample output from the **show ipv6 ospf interface** command when the OSPF graceful restart feature is configured:

```
Router# show ipv6 ospf interface

Ethernet0/0 is up, line protocol is up
  Link Local Address FE80::A8BB:CCFF:FE00:300, Interface ID 2
  Area 0, Process ID 1, Instance ID 0, Router ID 10.3.3.3
  Network Type POINT_TO_POINT, Cost: 10
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
   Graceful Restart p2p timeout in 00:00:19
    Hello due in 00:00:02
```

```
  Graceful Restart helper support enabled
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.1.1.1
  Suppress hello for 0 neighbor(s)
```

Example of an Enabled Protocol

The following display shows that the OSPF interface is enabled for Bidirectional Forwarding Detection (BFD):

```
Router# show ipv6 ospf interface

Serial10/0 is up, line protocol is up
  Link Local Address FE80::A8BB:CCFF:FE00:6500, Interface ID 42
  Area 1, Process ID 1, Instance ID 0, Router ID 10.0.0.1
  Network Type POINT_TO_POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT_TO_POINT, BFD enabled
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:07
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.1.0.1
  Suppress hello for 0 neighbor(s)
```

Related Commands

Command	Description
show ipv6 ospf graceful-restart	Displays OSPFv3 graceful restart information.

show ipv6 ospf neighbor

To display Open Shortest Path First (OSPF) neighbor information on a per-interface basis, use the **show ipv6 ospf neighbor** command in user EXEC or privileged EXEC mode.

show ipv6 ospf [*process-id*] [*area-id*] **neighbor** [*interface-type interface-number*] [*neighbor-id*] [**detail**]

Syntax Description

process-id	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when the OSPF routing process is enabled.
area-id	(Optional) Displays information only about a specified area.
interface-type interface-number	(Optional) Interface type and number.
neighbor-id	(Optional) Neighbor ID.
detail	(Optional) Displays all neighbors in detail (lists all neighbors).

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)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	Command output for the **detail** keyword was updated to display graceful-restart information.

Examples

The following is sample output from the **show ipv6 ospf neighbor** command:

```
Router# show ipv6 ospf neighbor

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
172.16.4.4        1   FULL/  -        00:00:31    14              POS4/0
172.16.3.3        1   FULL/BDR        00:00:30    3               FastEthernet00
172.16.5.5        1   FULL/  -        00:00:33    13              ATM3/0
```

The following is sample output from the **show ipv6 ospf neighbor** command with the **detail** keyword:

```
Router# show ipv6 ospf neighbor detail

 Neighbor 172.16.4.4
    In the area 0 via interface POS4/0
    Neighbor: interface-id 14, link-local address FE80::205:5FFF:FED3:5406
```

```
   Neighbor priority is 1, State is FULL, 6 state changes
   Options is 0x63AD1B0D
   Dead timer due in 00:00:33
   Neighbor is up for 00:48:56
   Index 1/1/1, retransmission queue length 0, number of retransmission 1
   First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
   Last retransmission scan length is 1, maximum is 1
   Last retransmission scan time is 0 msec, maximum is 0 msec
Neighbor 172.16.3.3
   In the area 1 via interface FastEthernet0/0
   Neighbor: interface-id 3, link-local address FE80::205:5FFF:FED3:5808
   Neighbor priority is 1, State is FULL, 6 state changes
   DR is 172.16.6.6 BDR is 172.16.3.3
   Options is 0x63F813E9
   Dead timer due in 00:00:33
   Neighbor is up for 00:09:00
   Index 1/1/2, retransmission queue length 0, number of retransmission 2
   First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
   Last retransmission scan length is 1, maximum is 2
   Last retransmission scan time is 0 msec, maximum is 0 msec
Neighbor 172.16.5.5
   In the area 2 via interface ATM3/0
   Neighbor: interface-id 13, link-local address FE80::205:5FFF:FED3:6006
   Neighbor priority is 1, State is FULL, 6 state changes
   Options is 0x63F7D249
   Dead timer due in 00:00:38
   Neighbor is up for 00:10:01
   Index 1/1/3, retransmission queue length 0, number of retransmission 0
   First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
   Last retransmission scan length is 0, maximum is 0
   Last retransmission scan time is 0 msec, maximum is 0 msec
```

Table 236 describes the significant fields shown in the display.

Table 236 show ipv6 ospf neighbor Field Descriptions

Field	Description
Neighbor ID; Neighbor	Neighbor router ID.
In the area	Area and interface through which the OSPF neighbor is known.
Pri; Neighbor priority	Router priority of the neighbor, neighbor state.
State	OSPF state.
State changes	Number of state changes since the neighbor was created.
Options	Hello packet options field contents. (E-bit only. Possible values are 0 and 2; 2 indicates area is not a stub; 0 indicates area is a stub.)
Dead timer due in	Expected time before Cisco IOS software will declare the neighbor dead.
Neighbor is up for	Number of hours:minutes:seconds since the neighbor went into two-way state.
Index	Neighbor location in the area-wide and autonomous system-wide retransmission queue.
retransmission queue length	Number of elements in the retransmission queue.

Table 236 show ipv6 ospf neighbor Field Descriptions (continued)

Field	Description
number of retransmission	Number of times update packets have been re-sent during flooding.
First	Memory location of the flooding details.
Next	Memory location of the flooding details.
Last retransmission scan length	Number of link state advertisements (LSAs) in the last retransmission packet.
maximum	Maximum number of LSAs sent in any retransmission packet.
Last retransmission scan time	Time taken to build last retransmission packet.
maximum	Maximum time taken to build any retransmission packet.

The following is sample output from the **show ipv6 ospf neighbor** command with the **detail** keyword, displaying graceful-restart information:

```
Router# show ipv6 ospf neighbor detail

 Neighbor 10.1.1.1
    In the area 0 via interface Ethernet0/0
    Neighbor: interface-id 3, link-local address FE80::A8BB:CCFF:FE00:200
    Neighbor priority is 1, State is FULL, 6 state changes
    DR is 10.1.1.1 BDR is 10.3.3.3
    Options is 0x1C9AD11
    Neighbor graceful restart timer due in 00:01:44
    Last neighbor graceful restart 01:00:19 ago
    Dead timer due in 00:00:36
    Neighbor is up for 00:00:16
    Index 1/1/1, retransmission queue length 0, number of retransmission 0
    First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
    Last retransmission scan length is 0, maximum is 0
    Last retransmission scan time is 0 msec, maximum is 0 msec
```

show ipv6 ospf request-list

To display a list of all link-state advertisements (LSAs) requested by a router, use the **show ipv6 ospf request-list** command in user EXEC or privileged EXEC mode.

show ipv6 ospf [*process-id*] [*area-id*] **request-list** [*neighbor*] [*interface*] [*interface-neighbor*]

Syntax Description

process-id	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when the Open Shortest Path First (OSPF) routing process is enabled.
area-id	(Optional) Displays information only about a specified area.
neighbor	(Optional) Displays the list of all LSAs requested by the router from this neighbor.
interface	(Optional) Displays the list of all LSAs requested by the router from this interface.
interface-neighbor	(Optional) Displays the list of all LSAs requested by the router on this interface, from this neighbor.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)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.

Usage Guidelines

The information displayed by the **show ipv6 ospf request-list** command is useful in debugging OSPF routing operations.

Examples

The following example shows information about the LSAs requested by the router:

```
Router# show ipv6 ospf request-list

            OSPFv3 Router with ID (192.168.255.5) (Process ID 1)

 Neighbor 192.168.255.2, interface Ethernet0/0 address
FE80::A8BB:CCFF:FE00:6600

 Type    LS ID           ADV RTR         Seq NO      Age    Checksum
  1      0.0.0.0         192.168.255.3   0x800000C2  1      0x0014C5
```

```
1       0.0.0.0         192.168.255.2   0x800000C8  0       0x000BCA
1       0.0.0.0         192.168.255.1   0x800000C5  1       0x008CD1
2       0.0.0.3         192.168.255.3   0x800000A9  774     0x0058C0
2       0.0.0.2         192.168.255.3   0x800000B7  1       0x003A63
```

Table 237 describes the significant fields shown in the display.

Table 237 show ipv6 ospf request-list Field Descriptions

Field	Description
OSPFv3 Router with ID (192.168.255.5) (Process ID 1)	Identification of the router for which information is displayed.
Interface Ethernet0/0	Interface for which information is displayed.
Type	Type of LSA.
LS ID	Link-state ID of the LSA.
ADV RTR	IP address of advertising router.
Seq NO	Sequence number of LSA.
Age	Age of LSA (in seconds).
Checksum	Checksum of LSA.

show ipv6 ospf retransmission-list

To display a list of all link-state advertisements (LSAs) waiting to be re-sent, use the **show ipv6 ospf retransmission-list** command in user EXEC or privileged EXEC mode.

show ipv6 ospf [*process-id*] [*area-id*] **retransmission-list** [*neighbor*] [*interface*] [*interface-neighbor*]

Syntax Description

process-id	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when the OSPF routing process is enabled.
area-id	(Optional) Displays information only about a specified area.
neighbor	(Optional) Displays the list of all LSAs waiting to be re-sent for this neighbor.
interface	(Optional) Displays the list of all LSAs waiting to be re-sent on this interface.
interface-neighbor	(Optional) Displays the list of all LSAs waiting to be re-sent on this interface, from this neighbor.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)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.

Usage Guidelines

The information displayed by the **show ipv6 ospf retransmission-list** command is useful in debugging Open Shortest Path First (OSPF) routing operations.

Examples

The following is sample output from the **show ipv6 ospf retransmission-list** command:

```
Router# show ipv6 ospf retransmission-list

        OSPFv3 Router with ID (192.168.255.2) (Process ID 1)

 Neighbor 192.168.255.1, interface Ethernet0/0
 Link state retransmission due in 3759 msec, Queue length 1

 Type    LS ID           ADV RTR         Seq NO      Age    Checksum
 0x2001  0               192.168.255.2   0x80000222  1      0x00AE52
```

Table 238 describes the significant fields shown in the display.

Table 238 show ipv6 ospf retransmission-list Field Descriptions

Field	Description
OSPFv3 Router with ID (192.168.255.2) (Process ID 1)	Identification of the router for which information is displayed.
Interface Ethernet0/0	Interface for which information is displayed.
Link state retransmission due in	Length of time before next link-state transmission.
Queue length	Number of elements in the retransmission queue.
Type	Type of LSA.
LS ID	Link-state ID of the LSA.
ADV RTR	IP address of advertising router.
Seq NO	Sequence number of the LSA.
Age	Age of LSA (in seconds).
Checksum	Checksum of LSA.

show ipv6 ospf statistics

To display Open Shortest Path First for IPv6 (OSPFv6) shortest path first (SPF) calculation statistics, use the **show ipv6 ospf statistics** command in user EXEC or privileged EXEC mode.

show ipv6 ospf statistics [**detail**]

Syntax Description

detail	(Optional) Displays statistics separately for each OSPF area and includes additional, more detailed statistics.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.

Usage Guidelines

The **show ipv6 ospf statistics** command provides important information about SPF calculations and the events that trigger them. This information can be meaningful for both OSPF network maintenance and troubleshooting. For example, entering the **show ipv6 ospf statistics** command is recommended as the first troubleshooting step for link-state advertisement (LSA) flapping.

Examples

The following example provides detailed statistics for each OSPFv6 area:

```
Router# show ipv6 ospf statistics detail

  Area 0: SPF algorithm executed 3 times

SPF 1 executed 00:06:57 ago, SPF type Full
  SPF calculation time (in msec):
  SPT    Prefix D-Int  Sum    D-Sum  Ext    D-Ext  Total
  0      0      0      0      0      0      0      0
  RIB manipulation time (in msec):
  RIB Update    RIB Delete
  0             0
  LSIDs processed R:1 N:0 Prefix:0 SN:0 SA:0 X7:0
  Change record R N SN SA L
  LSAs changed 1
  Changed LSAs. Recorded is Advertising Router, LSID and LS type:
  10.2.2.2/0(R)

SPF 2 executed 00:06:47 ago, SPF type Full
  SPF calculation time (in msec):
  SPT    Prefix D-Int  Sum    D-Sum  Ext    D-Ext  Total
  0      0      0      0      0      0      0      0
  RIB manipulation time (in msec):
  RIB Update    RIB Delete
  0             0
  LSIDs processed R:1 N:0 Prefix:1 SN:0 SA:0 X7:0
  Change record R L P
```

```
LSAs changed 4
Changed LSAs. Recorded is Advertising Router, LSID and LS type:
10.2.2.2/2(L) 10.2.2.2/0(R) 10.2.2.2/2(L) 10.2.2.2/0(P)
```

Table 205 describes the significant fields shown in the display.

Table 239 show ipv6 ospf statistics Field Descriptions

Field	Description
Area	OSPF area ID.
SPF	Number of SPF algorithms executed in the OSPF area. The number increases by one for each SPF algorithm that is executed in the area.
Executed ago	Time in milliseconds that has passed between the start of the SPF algorithm execution and the current time.
SPF type	SPF type can be Full or Incremental.
SPT	Time in milliseconds required to compute the first stage of the SPF algorithm (to build a short path tree). The SPT time plus the time required to process links to stub networks equals the Intra time.
Ext	Time in milliseconds for the SPF algorithm to process external and not so stubby area (NSSA) LSAs and to install external and NSSA routes in the routing table.
Total	Total duration time in milliseconds for the SPF algorithm process.
LSIDs processed	Number of LSAs processed during the SPF calculation: • N—Network LSA. • R—Router LSA. • SA—Summary Autonomous System Boundary Router (ASBR) (SA) LSA. • SN—Summary Network (SN) LSA. • Stub—Stub links. • X7—External Type-7 (X7) LSA.

show ipv6 ospf summary-prefix

To display a list of all summary address redistribution information configured under an OSPF process, use the **show ipv6 ospf summary-prefix** command in user EXEC or privileged EXEC mode.

show ipv6 ospf [*process-id*] **summary-prefix**

Syntax Description

process-id	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when the OSPF routing process is enabled.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)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.

Usage Guidelines

The *process-id* argument can be entered as a decimal number or as an IPv6 address format.

Examples

The following is sample output from the **show ipv6 ospf summary-prefix** command:

```
Router# show ipv6 ospf summary-prefix

OSPFv3 Process 1, Summary-prefix

FEC0::/24 Metric 16777215, Type 0, Tag 0
```

Table 240 describes the significant fields shown in the display.

Table 240 show ipv6 ospf summary-prefix Field Descriptions

Field	Description
OSPFv3 Process	Process ID of the router for which information is displayed.
Metric	Metric used to reach the destination router.
Type	Type of link-state advertisement (LSA).
Tag	LSA tag.

show ipv6 ospf timers rate-limit

To display all of the link-state advertisements (LSAs) in the rate limit queue, use the **show ipv6 ospf timers rate-limit** command in privileged EXEC mode.

show ipv6 ospf timers rate-limit

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

Use the **show ipv6 ospf timers rate-limit** command to discover when LSAs in the queue will be sent.

Examples

show ipv6 ospf timers rate-limit Output Example

The following is sample output from the **show ipv6 ospf timers rate-limit** command:

```
Router# show ipv6 ospf timers rate-limit

List of LSAs that are in rate limit Queue

    LSAID: 0.0.0.0 Type: 0x2001 Adv Rtr: 55.55.55.55 Due in: 00:00:00.500
    LSAID: 0.0.0.0 Type: 0x2009 Adv Rtr: 55.55.55.55 Due in: 00:00:00.500
```

Table 225 describes the significant fields shown in the display.

Table 241 show ipv6 ospf timers rate-limit Field Descriptions

Field	Description
LSAID	ID of the LSA.
Type	Type of LSA.
Adv Rtr	ID of the advertising router.
Due in:	When the LSA is scheduled to be sent (in hours:minutes:seconds).

show ipv6 ospf traffic

To display IPv6 Open Shortest Path First Version 3 (OSPFv3) traffic statistics, use the **show ipv6 ospf traffic** command in privileged EXEC mode.

show ipv6 ospf [*process-id*] **traffic** [*interface-type interface-number*]

Syntax Description

process-id	(Optional) OSPF process ID for which you want traffic statistics (for example, queue statistics, statistics for each interface under the OSPF process, and per OSPF process statistics).
interface-type interface-number	(Optional) Type and number associated with a specific OSPF interface.

Command Default

When the **show ipv6 ospf traffic** command is entered without any arguments, global OSPF traffic statistics are displayed, including queue statistics for each OSPF process, statistics for each interface, and per OSPF process statistics.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
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.

Usage Guidelines

You can limit the displayed traffic statistics to those for a specific OSPF process by entering a value for the *process-id* argument, or you can limit output to traffic statistics for a specific interface associated with an OSPF process by entering values for the *interface-type* and *interface-number* arguments. To reset counters and clear statistics, use the **clear ipv6 ospf traffic** command.

Examples

The following example shows the display output for the **show ipv6 ospf traffic** command for OSPFv3:

```
Router# show ipv6 ospf traffic

OSPFv3 statistics:
  Rcvd: 32 total, 0 checksum errors
        10 hello, 7 database desc, 2 link state req
        9 link state updates, 4 link state acks
        0 LSA ignored

  Sent: 45 total, 0 failed
        17 hello, 12 database desc, 2 link state req
        8 link state updates, 6 link state acks
```

```
        OSPFv3 Router with ID (10.1.1.4) (Process ID 6)

OSPFv3 queues statistic for process ID 6
  Hello queue size 0, no limit, max size 2
  Router queue size 0, limit 200, drops 0, max size 2


Interface statistics:


    Interface Serial2/0

OSPFv3 packets received/sent

  Type          Packets              Bytes
  RX Invalid    0                    0
  RX Hello      5                    196
  RX DB des     4                    172
  RX LS req     1                    52
  RX LS upd     4                    320
  RX LS ack     2                    112
  RX Total      16                   852

  TX Failed     0                    0
  TX Hello      8                    304
  TX DB des     3                    144
  TX LS req     1                    52
  TX LS upd     3                    252
  TX LS ack     3                    148
  TX Total      18                   900

OSPFv3 header errors
  Length 0, Checksum 0, Version 0, No Virtual Link 0,
  Area Mismatch 0, Self Originated 0, Duplicate ID 0,
  Instance ID 0, Hello 0, MTU Mismatch 0,
  Nbr Ignored 0, Authentication 0,

OSPFv3 LSA errors
  Type 0, Length 0, Data 0, Checksum 0,


    Interface Ethernet0/0

OSPFv3 packets received/sent

  Type          Packets              Bytes
  RX Invalid    0                    0
  RX Hello      6                    240
  RX DB des     3                    144
  RX LS req     1                    52
  RX LS upd     5                    372
  RX LS ack     2                    152
  RX Total      17                   960

  TX Failed     0                    0
  TX Hello      11                   420
  TX DB des     9                    312
  TX LS req     1                    52
  TX LS upd     5                    376
  TX LS ack     3                    148
  TX Total      29                   1308

OSPFv3 header errors
```

```
  Length 0, Checksum 0, Version 0, No Virtual Link 0,
  Area Mismatch 0, Self Originated 0, Duplicate ID 0,
  Instance ID 0, Hello 0, MTU Mismatch 0,
  Nbr Ignored 0, Authentication 0,

OSPFv3 LSA errors
  Type 0, Length 0, Data 0, Checksum 0,


Summary traffic statistics for process ID 6:

OSPFv3 packets received/sent

  Type          Packets              Bytes
  RX Invalid    0                    0
  RX Hello      11                   436
  RX DB des     7                    316
  RX LS req     2                    104
  RX LS upd     9                    692
  RX LS ack     4                    264
  RX Total      33                   1812

  TX Failed     0                    0
  TX Hello      19                   724
  TX DB des     12                   456
  TX LS req     2                    104
  TX LS upd     8                    628
  TX LS ack     6                    296
  TX Total      47                   2208

OSPFv3 header errors
  Length 0, Checksum 0, Version 0, No Virtual Link 0,
  Area Mismatch 0, Self Originated 0, Duplicate ID 0,
  Instance ID 0, Hello 0, MTU Mismatch 0,
  Nbr Ignored 0, Authentication 0,

OSPFv3 LSA errors
  Type 0, Length 0, Data 0, Checksum 0,
```

The network administrator wants to start collecting new statistics, resetting the counters and clearing the traffic statistics by entering the **clear ipv6 ospf traffic** command as follows:

```
Router# clear ipv6 ospf traffic
```

Table 242 describes the significant fields shown in the display.

Table 242 show ipv6 ospf traffic Field Descriptions

Field	Description
OSPFv3 statistics	Traffic statistics accumulated for all OSPF processes running on the router. To ensure compatibility with the **show ip traffic** command, only checksum errors are displayed. Identifies the route map name.
OSPFv3 queues statistic for process ID	Queue statistics specific to Cisco IOS software.
Hello queue	Statistics for the internal Cisco IOS queue between the packet switching code (process IP Input) and the OSPF hello process for all received OSPF packets.

Table 242 show ipv6 ospf traffic Field Descriptions (continued)

Field	Description
Router queue	Statistics for the internal Cisco IOS queue between the OSPF hello process and the OSPF router for all received OSPF packets except OSPF hellos.
queue size	Actual size of the queue.
queue limit	Maximum allowed size of the queue.
queue max size	Maximum recorded size of the queue.
Interface statistics	Per-interface traffic statistics for all interfaces that belong to the specific OSPFv3 process ID.
OSPFv3 packets received/sent	Number of OSPFv3 packets received and sent on the interface, sorted by packet types.
OSPFv3 header errors	Packet appears in this section if it was discarded because of an error in the header of an OSPFv3 packet. The discarded packet is counted under the appropriate discard reason.
OSPFv3 LSA errors	Packet appears in this section if it was discarded because of an error in the header of an OSPF link-state advertisement (LSA). The discarded packet is counted under the appropriate discard reason.
Summary traffic statistics for process ID	Summary traffic statistics accumulated for an OSPFv3 process. **Note** The OSPF process ID is a unique value assigned to the OSPFv3 process in the configuration. The value for the received errors is the sum of the OSPFv3 header errors that are detected by the OSPFv3 process, unlike the sum of the checksum errors that are listed in the global OSPF statistics.

Related Commands

Command	Description
clear ip ospf traffic	Clears OSPFv2 traffic statistics.
clear ipv6 ospf traffic	Clears OSPFv3 traffic statistics.
show ip ospf traffic	Displays OSPFv2 traffic statistics.

show ipv6 ospf virtual-links

To display parameters and the current state of Open Shortest Path First (OSPF) virtual links, use the **show ipv6 ospf virtual-links** command in user EXEC or privileged EXEC mode.

show ipv6 ospf virtual-links

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)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.
12.4(9)T	Command output was updated to display OSPF for IPv6 encryption information.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The information displayed by the **show ipv6 ospf virtual-links** command is useful in debugging OSPF routing operations.

Examples

The following is sample output from the **show ipv6 ospf virtual-links** command:

```
Router# show ipv6 ospf virtual-links

Virtual Link OSPF_VL0 to router 172.16.6.6 is up
  Interface ID 27, IPv6 address FEC0:6666:6666::
  Run as demand circuit
  DoNotAge LSA allowed.
  Transit area 2, via interface ATM3/0, Cost of using 1
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
```

Table 243 describes the significant fields shown in the display.

Table 243 show ipv6 ospf virtual-links Field Descriptions

Field	Description
Virtual Link OSPF_VL0 to router 172.16.6.6 is up	Specifies the OSPF neighbor, and if the link to that neighbor is up or down.
Interface ID	Interface ID and IPv6 address of the router.
Transit area 2	The transit area through which the virtual link is formed.
via interface ATM3/0	The interface through which the virtual link is formed.
Cost of using 1	The cost of reaching the OSPF neighbor through the virtual link.
Transmit Delay is 1 sec	The transmit delay (in seconds) on the virtual link.
State POINT_TO_POINT	The state of the OSPF neighbor.
Timer intervals...	The various timer intervals configured for the link.
Hello due in 0:00:06	When the next hello is expected from the neighbor.

The following sample output from the **show ipv6 ospf virtual-links** command has two virtual links. One is protected by authentication, and the other is protected by encryption.

```
Router# show ipv6 ospf virtual-links

Virtual Link OSPFv3_VL1 to router 10.2.0.1 is up
   Interface ID 69, IPv6 address 2001:0DB8:11:0:A8BB:CCFF:FE00:6A00
   Run as demand circuit
   DoNotAge LSA allowed.
   Transit area 1, via interface Serial12/0, Cost of using 64
   NULL encryption SHA-1 auth SPI 3944, secure socket UP (errors: 0)
   Transmit Delay is 1 sec, State POINT_TO_POINT,
   Timer intervals configured, Hello 2, Dead 10, Wait 40, Retransmit 5
     Adjacency State FULL (Hello suppressed)
     Index 1/2/4, retransmission queue length 0, number of retransmission 1
     First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
     Last retransmission scan length is 1, maximum is 1
     Last retransmission scan time is 0 msec, maximum is 0 msec
Virtual Link OSPFv3_VL0 to router 10.1.0.1 is up
   Interface ID 67, IPv6 address 2001:0DB8:13:0:A8BB:CCFF:FE00:6700
   Run as demand circuit
   DoNotAge LSA allowed.
   Transit area 1, via interface Serial11/0, Cost of using 128
   MD5 authentication SPI 940, secure socket UP (errors: 0)
   Transmit Delay is 1 sec, State POINT_TO_POINT,
   Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
     Adjacency State FULL (Hello suppressed)
     Index 1/1/3, retransmission queue length 0, number of retransmission 1
First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
     Last retransmission scan length is 1, maximum is 1
     Last retransmission scan time is 0 msec, maximum is 0 msec
```

show ipv6 pim bsr

To display information related to Protocol Independent Multicast (PIM) bootstrap router (BSR) protocol processing, use the **show ipv6 pim bsr** command in user EXEC or privileged EXEC mode.

show ipv6 pim [**vrf** *vrf-name*] **bsr** {**election** | **rp-cache** | **candidate-rp**}

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
election	Displays BSR state, BSR election, and bootstrap message (BSM)-related timers.
rp-cache	Displays candidate rendezvous point (C-RP) cache learned from unicast C-RP announcements on the elected BSR.
candidate-rp	Displays C-RP state on routers that are configured as C-RPs.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.0(28)S	The **election**, **rp-cache**, and **candidate-rp** keywords were added.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(11)T	The **election**, **rp-cache**, and **candidate-rp** keywords 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.
12.2(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 introduced on Cisco ASR 1000 Series Routers.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

Use the **show ipv6 pim bsr** command to display details of the BSR election-state machine, C-RP advertisement state machine, and the C-RP cache. Information on the C-RP cache is displayed only on the elected BSR router, and information on the C-RP state machine is displayed only on a router configured as a C-RP.

Examples

The following example displays BSM election information:

```
Router# show ipv6 pim bsr election

PIMv2 BSR information
BSR Election Information
```

```
Scope Range List: ff00::/8
This system is the Bootstrap Router (BSR)
BSR Address: 60::1:1:4
Uptime: 00:11:55, BSR Priority: 0, Hash mask length: 126
RPF: FE80::A8BB:CCFF:FE03:C400,Ethernet0/0
BS Timer: 00:00:07
This system is candidate BSR
Candidate BSR address: 60::1:1:4, priority: 0, hash mask length: 126
```

Table 243 describes the significant fields shown in the display.

Table 244 show ipv6 pim bsr election Field Descriptions

Field	Description
Scope Range List	Scope to which this BSR information applies.
This system is the Bootstrap Router (BSR)	Indicates this router is the BSR and provides information on the parameters associated with it.
BS Timer	On the elected BSR, the BS timer shows the time in which the next BSM will be originated. On all other routers in the domain, the BS timer shows the time at which the elected BSR expires.
This system is candidate BSR	Indicates this router is the candidate BSR and provides information on the parameters associated with it.

The following example displays information that has been learned from various C-RPs at the BSR. In this example, two candidate RPs have sent advertisements for the FF00::/8 or the default IPv6 multicast range:

```
Router# show ipv6 pim bsr rp-cache

PIMv2 BSR C-RP Cache
BSR Candidate RP Cache
Group(s) FF00::/8, RP count 2
  RP 10::1:1:3
    Priority 192, Holdtime 150
    Uptime: 00:12:36, expires: 00:01:55
  RP 20::1:1:1
    Priority 192, Holdtime 150
    Uptime: 00:12:36, expires: 00:01:5
```

The following example displays information about the C-RP. This RP has been configured without a specific scope value, so the RP will send C-RP advertisements to all BSRs about which it has learned through BSMs it has received.

```
Router# show ipv6 pim bsr candidate-rp

PIMv2 C-RP information
    Candidate RP: 10::1:1:3
      All Learnt Scoped Zones, Priority 192, Holdtime 150
      Advertisement interval 60 seconds
      Next advertisement in 00:00:33
```

show ipv6 pim df

To display the designated forwarder (DF)-election state of each interface for each rendezvous point (RP), use the **show ipv6 pim df** command in user EXEC or privileged EXEC mode.

show ipv6 pim [**vrf** *vrf-name*] **df** [*interface-type interface-number*] [*rp-address*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
interface-type interface-number	(Optional) Interface type and number. For more information, use the question mark (?) online help function.
rp-address	(Optional) RP IPv6 address.

Command Default

If no interface or RP address is specified, all DFs are displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
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.
12.2(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 introduced on Cisco ASR 1000 Series Routers.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

Use the **show ipv6 pim df** command to display the state of the DF election for each RP on each Protocol Independent Multicast (PIM)-enabled interface if the bidirectional multicast traffic is not flowing as expected.

Examples

The following example displays the DF-election states:

```
Router# show ipv6 pim df

Interface          DF State     Timer         Metrics
Ethernet0/0        Winner       4s 8ms        [120/2]
    RP :200::1
Ethernet1/0        Lose         0s 0ms        [inf/inf]
    RP :200::1
```

The following example shows information on the RP:

```
Router# show ipv6 pim df

Interface          DF State     Timer         Metrics
Ethernet0/0        None:RP LAN 0s 0ms        [inf/inf]
    RP :200::1
Ethernet1/0        Winner       7s 600ms      [0/0]
    RP :200::1
Ethernet2/0        Winner       9s 8ms        [0/0]
    RP :200::1
```

Table 245 describes the significant fields shown in the display.

Table 245 show ipv6 pim df Field Descriptions

Field	Description
Interface	Interface type and number that is configured to run PIM.
DF State	The state of the DF election on the interface. The state can be: • Offer • Winner • Backoff • Lose • None:RP LAN The None:RP LAN state indicates that no DF election is taking place on this LAN because the RP is directly connected to this LAN.
Timer	DF election timer.
Metrics	Routing metrics to the RP announced by the DF.
RP	The IPv6 address of the RP.

Related Commands

Command	Description
debug ipv6 pim df-election	Displays debug messages for PIM bidirectional DF-election message processing.
ipv6 pim rp-address	Configures the address of a PIM RP for a particular group range.
show ipv6 pim df winner	Displays the DF-election winner on each interface for each RP.

show ipv6 pim df winner

To display the designated forwarder (DF)-election winner on each interface for each rendezvous point (RP), use the **show ipv6 pim df winner** command in user EXEC or privileged EXEC mode.

show ipv6 pim [**vrf** *vrf-name*] **df winner** [*interface-type interface-number*] [*rp-address*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
interface-type interface-number	(Optional) Interface type and number. For more information, use the question mark (?) online help function.
rp-address	(Optional) RP IPv6 address.

Command Default

If no interface or RP address is specified, all DFs are displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
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.
12.2(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 introduced on Cisco ASR 1000 Series Routers.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

Use the **show ipv6 pim df winner** command to display the DF election winner for each RP on each Protocol Independent Multicast (PIM)-enabled interface if the bidirectional multicast traffic is not flowing as expected.

Examples

The following example shows the DF winner for the IPv6 address 200::1:

```
Router# show ipv6 pim df winner ethernet 1/0 200::1

Interface          Metrics
Ethernet1/0        [120/2]
RP        : 200::1
DF Winner : FE80::A8BB:CCFF:FE00:601
```

Table 245 describes the significant fields shown in the display.

Table 246 show ipv6 pim df winner Field Descriptions

Field	Description
Interface	Interface type and number that is configured to run PIM.
Metrics	Routing metrics to the RP announced by the DF.
RP	The IPv6 address of the RP.
DF Winner	The IPv6 address of the DF election winner.

Related Commands

Command	Description
debug ipv6 pim df-election	Displays debug messages for PIM bidirectional DF-election message processing.
ipv6 pim rp-address	Configures the address of a PIM RP for a particular group range.
show ipv6 pim df	Displays the DF -election state of each interface for each RP.

show ipv6 pim group-map

To display an IPv6 Protocol Independent Multicast (PIM) group mapping table, use the **show ipv6 pim group-map** command in user EXEC or privileged EXEC mode.

show ipv6 pim [**vrf** *vrf-name*] **group-map** [*group-name* | *group-address*] | [*group-range* | *group-mask*] [**info-source** {**bsr** | **default** | **embedded-rp** | **static**}]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
group-name | *group-address*	(Optional) IPv6 address or name of the multicast group.
group-range | *group-mask*	(Optional) Group range list. Includes group ranges with the same prefix or mask length.
info-source	(Optional) Displays all mappings learned from a specific source, such as the bootstrap router (BSR) or static configuration.
bsr	Displays ranges learned through the BSR.
default	Displays ranges enabled by default.
embedded-rp	Displays group ranges learned through the embedded rendezvous point (RP).
static	Displays ranges enabled by static configuration.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.0(28)S	The *group-range* and *group-mask* arguments were added, and the **info-source bsr**, **static**, and **default** keywords were added.
12.2(25)S	The *group-range* and *group-mask* arguments were added, and the **info-source bsr**, **static**, and **default** keywords were added.
12.3(11)T	The *group-range* and *group-mask* arguments were added, and the **info-source bsr**, **static**, and **default** keywords 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.
12.2(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(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

Use the **show ipv6 pim group-map** command to find all group mappings installed by a given source of information, such as BSR or static configuration.

You can also use this command to find which group mapping a router at a specified IPv6 group address is using by specifying a group address, or to find an exact group mapping entry by specifying a group range and mask length.

Examples

The following is sample output from the **show ipv6 pim group-map** command:

```
Router# show ipv6 pim group-map

FF33::/32*
      SSM
      Info source:Static
      Uptime:00:08:32, Groups:0
  FF34::/32*
      SSM
      Info source:Static
      Uptime:00:09:42, Groups:0
```

Table 247 describes the significant fields shown in the display.

Table 247 show ipv6 pim group-map Field Descriptions

Field	Description
RP	Address of the RP router if the protocol is sparse mode or bidir.
Protocol	Protocol used: sparse mode (SM), Source Specific Multicast (SSM), link-local (LL), or NOROUTE (NO). LL is used for the link-local scoped IPv6 address range (ff[0-f]2::/16). LL is treated as a separate protocol type, because packets received with these destination addresses are not forwarded, but the router might need to receive and process them. NOROUTE or NO is used for the reserved and node-local scoped IPv6 address range (ff[0-f][0-1]::/16). These addresses are nonroutable, and the router does not need to process them.
Groups	How many groups are present in the topology table from this range.
Info source	Mappings learned from a specific source; in this case, static configuration.
Uptime	The uptime for the group mapping displayed.

The following example displays the group mappings learned from BSRs that exist in the PIM group-to-RP or mode-mapping cache. The example shows the address of the BSR from which the group mappings have been learned and the associated timeout.

```
Router# show ipv6 pim group-map info-source bsr

FF00::/8*
    SM, RP: 20::1:1:1
    RPF: Et1/0,FE80::A8BB:CCFF:FE03:C202
    Info source: BSR From: 60::1:1:4(00:01:42), Priority: 192
    Uptime: 00:19:51, Groups: 0
FF00::/8*
    SM, RP: 10::1:1:3
    RPF: Et0/0,FE80::A8BB:CCFF:FE03:C102
    Info source: BSR From: 60::1:1:4(00:01:42), Priority: 192
    Uptime: 00:19:51, Groups: 0
```

show ipv6 pim interface

To display information about interfaces configured for Protocol Independent Multicast (PIM), use the **show ipv6 pim interface** command in privileged EXEC mode.

show ipv6 pim [**vrf** *vrf-name*] **interface** [**state-on**] [**state-off**] [*type number*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
state-on	(Optional) Displays interfaces with PIM enabled.
state-off	(Optional) Displays interfaces with PIM disabled.
type number	(Optional) Interface type and number.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	The **state-on** and **state-off** keywords were added.
12.3(4)T	The **state-on** and **state-off** keywords 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.
12.2(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(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

The **show ipv6 pim interface** command is used to check if PIM is enabled on an interface, the number of neighbors, and the designated router (DR) on the interface.

Examples

The following is sample output from the **show ipv6 pim interface** command using the **state-on** keyword:

```
Router# show ipv6 pim interface state-on

Interface          PIM  Nbr   Hello  DR
                        Count Intvl  Prior

Ethernet0          on   0     30     1
    Address:FE80::208:20FF:FE08:D7FF
    DR     :this system
POS1/0             on   0     30     1
    Address:FE80::208:20FF:FE08:D554
    DR     :this system
POS4/0             on   1     30   1
    Address:FE80::208:20FF:FE08:D554
```

```
    DR     :FE80::250:E2FF:FE8B:4C80
POS4/1             on   0     30   1
    Address:FE80::208:20FF:FE08:D554
    DR     :this system
Loopback0          on   0     30     1
    Address:FE80::208:20FF:FE08:D554
    DR     :this system
```

Table 248 describes the significant fields shown in the display.

Table 248 show ipv6 pim interface Field Descriptions

Field	Description
Interface	Interface type and number that is configured to run PIM.
PIM	Whether PIM is enabled on an interface.
Nbr Count	Number of PIM neighbors that have been discovered through this interface.
Hello Intvl	Frequency, in seconds, of PIM hello messages.
DR	IP address of the designated router (DR) on a network.
Address	Interface IP address of the next-hop router.

Related Commands

Command	Description
show ipv6 pim neighbor	Displays the PIM neighbors discovered by the Cisco IOS software.

show ipv6 pim join-prune statistic

To display the average join-prune aggregation for the most recently aggregated 1000, 10,000, and 50,000 packets for each interface, use the **show ipv6 pim join-prune statistic** command in user EXEC or privileged EXEC mode.

show ipv6 pim [**vrf** *vrf-name*] **join-prune statistic** [*interface-type*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
interface-type	(Optional) Interface type. For more information, use the question mark (**?**) online help function.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.3(4)T	This command was 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(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

When Protocol Independent Multicast (PIM) sends multiple joins and prunes simultaneously, it aggregates them into a single packet. The **show ipv6 pim join-prune statistic** command displays the average number of joins and prunes that were aggregated into a single packet over the last 1000 PIM join-prune packets, over the last 10,000 PIM join-prune packets, and over the last 50,000 PIM join-prune packets.

Examples

The following example provides the join/prune aggregation on Ethernet interface 0/0/0:

```
Router# show ipv6 pim join-prune statistic Ethernet0/0/0

PIM Average Join/Prune Aggregation for last (1K/10K/50K) packets
Interface             Transmitted             Received

Ethernet0/0/0      0    / 0    / 0         1    / 0    / 0
```

Table 249 describes the significant fields shown in the display.

Table 249 show ipv6 pim join-prune statistics Field Descriptions

Field	Description
Interface	The interface from which the specified packets were transmitted or on which they were received.
Transmitted	The number of packets transmitted on the interface.
Received	The number of packets received on the interface.

show ipv6 pim limit

To display Protocol Independent Multicast (PIM) interface limit, use the **show ipv6 pim limit** command in privileged EXEC mode.

show ipv6 pim [**vrf** *vrf-name*] **limit** [*interface*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
interface	(Optional) Specific interface for which limit information is provided.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

The **show ipv6 pim limit** command checks interface statistics for limits. If the optional *interface* argument is enabled, only information for the specified interface is shown.

Examples

The following example displays s PIM interface limit information:

```
Router# show ipv6 pim limit
```

Related Commands

Command	Description
ipv6 multicast limit	Configures per-interface mroute state limiters in IPv6.
ipv6 multicast limit cost	Applies a cost to mroutes that match per interface mroute state limiters in IPv6.

show ipv6 pim limit

To display Protocol Independent Multicast (PIM) interface limit, use the **show ipv6 pim limit** command in privileged EXEC mode.

show ipv6 pim [**vrf** *vrf-name*] **limit** [*interface*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
interface	(Optional) Specific interface for which limit information is provided.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

The **show ipv6 pim limit** command checks interface statistics for limits. If the optional *interface* argument is enabled, only information for the specified interface is shown.

Examples

The following example displays s PIM interface limit information:

```
Router# show ipv6 pim limit
```

Related Commands

Command	Description
ipv6 multicast limit	Configures per-interface mroute state limiters in IPv6.
ipv6 multicast limit cost	Applies a cost to mroutes that match per interface mroute state limiters in IPv6.

show ipv6 pim range-list

To display information about IPv6 multicast range lists, use the **show ipv6 pim range-list** command in privileged EXEC mode.

show ipv6 pim [**vrf** *vrf-name*] **range-list** [**config**] [*rp-address* | *rp-name*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
config	(Optional) The client. Displays the range lists configured on the router.
rp-address | *rp-name*	(Optional) The address of a Protocol Independent Multicast (PIM) rendezvous point (RP).

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
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.
12.2(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(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

The **show ipv6 pim range-list** command displays IPv6 multicast range lists on a per-client and per-mode basis. A client is the entity from which the specified range list was learned. The clients can be config, and the modes can be Source Specific Multicast (SSM) or sparse mode (SM).

Examples

The following is sample output from the **show ipv6 pim range-list** command:

```
Router# show ipv6 pim range-list

config SSM Exp:never Learnt from :::
 FF33::/32 Up:00:26:33
 FF34::/32 Up:00:26:33
 FF35::/32 Up:00:26:33
 FF36::/32 Up:00:26:33
 FF37::/32 Up:00:26:33
 FF38::/32 Up:00:26:33
 FF39::/32 Up:00:26:33
 FF3A::/32 Up:00:26:33
 FF3B::/32 Up:00:26:33
 FF3C::/32 Up:00:26:33
 FF3D::/32 Up:00:26:33
 FF3E::/32 Up:00:26:33
```

```
 FF3F::/32 Up:00:26:33
config SM RP:40::1:1:1 Exp:never Learnt from :::
 FF13::/64 Up:00:03:50
config SM RP:40::1:1:3 Exp:never Learnt from :::
 FF09::/64 Up:00:03:50
```

Table 250 describes the significant fields shown in the display.

Table 250 show ipv6 pim range-list Field Descriptions

Field	Description
config	Config is the client.
SSM	Protocol being used.
FF33::/32	Group range.
Up:	Uptime.

show ipv6 pim topology

To display Protocol Independent Multicast (PIM) topology table information for a specific group or all groups, use the **show ipv6 pim topology** command in user EXEC or privileged EXEC mode.

show ipv6 pim [**vrf** *vrf-name*] **topology** [*groupname-or-address* [*sourcename-or-address*] | **link-local** | **route-count** [**detail**]]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
groupname-or-address	(Optional) IPv6 address or name of the multicast group.
sourcename-or-address	(Optional) IPv6 address or name of the source.
link-local	(Optional) Displays the link-local groups.
route-count	(Optional) Displays the number of routes in PIM topology table.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was modified. The **link-local** keyword was added.
12.3(4)T	This command was modified. The **link-local** keyword was 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.
12.2(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 introduced on Cisco ASR 1000 Series Routers.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

This command shows the PIM topology table for a given group—(*, G), (S, G), and (S, G) Rendezvous Point Tree (RPT)— as internally stored in a PIM topology table. The PIM topology table may have various entries for a given group, each with its own interface list. The resulting forwarding state is maintained in the Multicast Routing Information Base (MRIB) table, which shows which interface the data packet should be accepted on and which interfaces the data packet should be forwarded to for a given (S, G) entry. Additionally, the Multicast Forwarding Information Base (MFIB) table is used during forwarding to decide on per-packet forwarding actions.

The **route-count** keyword shows the count of all entries, including link-local entries.

PIM communicates the contents of these entries through the MRIB, which is an intermediary for communication between multicast routing protocols (such as PIM), local membership protocols (such as Multicast Listener Discovery [MLD]), and the multicast forwarding engine of the system.

For example, an interface is added to the (*, G) entry in PIM topology table upon receipt of an MLD report or PIM (*, G) join message. Similarly, an interface is added to the (S, G) entry upon receipt of the MLD INCLUDE report for the S and G or PIM (S, G) join message. Then PIM installs an (S, G) entry in the MRIB with the immediate olist (from (S, G)) and the inherited olist (from (*, G)). Therefore, the proper forwarding state for a given entry (S, G) can be seen only in the MRIB or the MFIB, not in the PIM topology table.

Examples

The following is sample output from the **show ipv6 pim topology** command:

```
Router# show ipv6 pim topology

IP PIM Multicast Topology Table
Entry state:(*/S,G)[RPT/SPT] Protocol Uptime Info
Entry flags:KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive,
    RA - Really Alive, LH - Last Hop, DSS - Don't Signal Sources,
    RR - Register Received, SR - Sending Registers, E - MSDP External,
    DCC - Don't Check Connected
Interface state:Name, Uptime, Fwd, Info
Interface flags:LI - Local Interest, LD - Local Dissinterest,
II - Internal Interest, ID - Internal Dissinterest,
LH - Last Hop, AS - Assert, AB - Admin Boundary

(*,FF05::1)
SM UP:02:26:56 JP:Join(now) Flags:LH
RP:40::1:1:2
RPF:Ethernet1/1,FE81::1
  Ethernet0/1          02:26:56  fwd LI LH

(50::1:1:200,FF05::1)
SM UP:00:00:07 JP:Null(never) Flags:
RPF:Ethernet1/1,FE80::30:1:4
  Ethernet1/1          00:00:07  off LI
```

Table 251 describes the significant fields shown in the display.

Table 251 show ipv6 pim topology Field Descriptions

Field	Description
Entry flags: KAT	The keepalive timer (KAT) associated with a source is used to keep track of two intervals while the source is alive. When a source first becomes active, the first-hop router sets the keepalive timer to 3 minutes and 30 seconds, during which time it does not probe to see if the source is alive. Once this timer expires, the router enters the probe interval and resets the timer to 65 seconds, during which time the router assumes the source is alive and starts probing to determine if it actually is. If the router determines that the source is alive, the router exits the probe interval and resets the keepalive timer to 3 minutes and 30 seconds. If the source is not alive, the entry is deleted at the end of the probe interval.
AA, PA	The assume alive (AA) and probe alive (PA) flags are set when the router is in the probe interval for a particular source.
RR	The register received (RR) flag is set on the (S, G) entries on the Route Processor (RP) as long as the RP receives registers from the source Designated Router (DR), which keeps the source state alive on the RP.
SR	The sending registers (SR) flag is set on the (S, G) entries on the DR as long as it sends registers to the RP.

Related Commands

Command	Description
show ipv6 mrib client	Displays information about the clients of the MRIB.
show ipv6 mrib route	Displays MRIB route information.

show ipv6 pim traffic

To display the Protocol Independent Multicast (PIM) traffic counters, use the **show ipv6 pim traffic** command in user EXEC or privileged EXEC mode.

show ipv6 pim [**vrf** *vrf-name*] **traffic**

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.3(4)T	This command was 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(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

Use the **show ipv6 pim traffic** command to check if the expected number of PIM protocol messages have been received and sent.

Examples

The following example shows the number of PIM protocol messages received and sent.

```
Router# show ipv6 pim traffic

PIM Traffic Counters
Elapsed time since counters cleared:00:05:29

                              Received     Sent
Valid PIM Packets               22          22
Hello                           22          22
Join-Prune                      0           0
Register                        0           0
Register Stop                   0           0
Assert                          0           0
Bidir DF Election               0           0

Errors:
Malformed Packets                           0
Bad Checksums                               0
Send Errors                                 0
Packet Sent on Loopback Errors              0
Packets Received on PIM-disabled Interface  0
Packets Received with Unknown PIM Version   0
```

Table 252 describes the significant fields shown in the display.

Table 252 show ipv6 pim traffic Field Descriptions

Field	Description
Elapsed time since counters cleared	Indicates the amount of time (in hours, minutes, and seconds) since the counters cleared.
Valid PIM Packets	Number of valid PIM packets received and sent.
Hello	Number of valid hello messages received and sent.
Join-Prune	Number of join and prune announcements received and sent.
Register	Number of PIM register messages received and sent.
Register Stop	Number of PIM register stop messages received and sent.
Assert	Number of asserts received and sent.

show ipv6 pim tunnel

To display information about the Protocol Independent Multicast (PIM) register encapsulation and de-encapsulation tunnels on an interface, use the **show ipv6 pim tunnel** command in privileged EXEC mode.

show ipv6 pim [**vrf** *vrf-name*] **tunnel** [*interface-type interface-number*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
interface-type interface-number	(Optional) Tunnel interface type and number.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
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.
12.2(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(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

If you use the **show ipv6 pim tunnel** command without the optional *interface* keyword, information about the PIM register encapsulation and de-encapsulation tunnel interfaces is displayed.

The PIM encapsulation tunnel is the register tunnel. An encapsulation tunnel is created for every known rendezvous point (RP) on each router. The PIM decapsulation tunnel is the register decapsulation tunnel. A decapsulation tunnel is created on the RP for the address that is configured to be the RP address.

Examples

The following is sample output from the **show ipv6 pim tunnel** command on the RP:

```
Router# show ipv6 pim tunnel

Tunnel0*
 Type  :PIM Encap
 RP    :100::1
 Source:100::1
Tunnel0*
 Type  :PIM Decap
 RP    :100::1
 Source: -
```

The following is sample output from the **show ipv6 pim tunnel** command on a non-RP:

```
Router# show ipv6 pim tunnel

Tunnel0*
 Type  :PIM Encap
 RP    :100::1
 Source:2001::1:1:1
```

Table 253 describes the significant fields shown in the display.

Table 253 show ipv6 pim tunnel Field Descriptions

Field	Description
Tunnel0*	Name of the tunnel.
Type	Type of tunnel. Can be PIM encapsulation or PIM de-encapsulation.
source	Source address of the router that is sending encapsulating registers to the RP.

show ipv6 policy

To display IPv6 policy-based routing (PBR) configuration, use the **show ipv6 policy** command in user EXEC or privileged EXEC mode.

show ipv6 policy

Syntax Description

This command has no arguments or keywords.

Command Default

PBR configuration is not displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(33)SXI4	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SXI4.
Cisco IOS XE Release 3.2S	This command was modified. It was integrated into Cisco IOS XE Release 3.2S.

Usage Guidelines

IPv6 policy matches will be counted on route maps, as is done in IP version 4. Therefore, IPv6 policy matches can also be displayed on the **show route-map** command.

Examples

The following example displays the PBR configuration:

```
Router# show ipv6 policy

Interface                Routemap
Ethernet0/0              src-1
```

Table 245 describes the significant fields shown in the display.

Table 254 show ipv6 policy Field Descriptions

Field	Description
Interface	Interface type and number that is configured to run PIM.
Routemap	The name of the route map on which IPv6 policy matches were counted.

Related Commands

Command	Description
show route-map	Displays all route maps configured or only the one specified.

show ipv6 port-map

To verify port-to-application mapping (PAM) configuration, use the **show ipv6 port-map** command in user EXEC or privileged EXEC mode.

show ipv6 port-map [*application* | **port** *port-number*]

Syntax Description

application	(Optional) Specifies the name of the application used in port mapping.
port *port-number*	(Optional) Specifies the port number that maps to the application.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(11)T	This command was introduced.

Usage Guidelines

The **show ipv6 port-map** command displays the entire IPv6 port-mapping table or specific port-mapping information of a particular port number or application (protocol). Enabling the **show ipv6 port-map** command displays the entire IPv6 PAM table, including system-defined, user-defined, and host-specific port-mapping configurations.

To display port-mapping details of a specific port number, use the **show ipv6 port-map** command with the **port** *port-number* keyword and argument.

To display the port-mapping details of a specific application, use the **show ipv6 port-map** command with the *application* argument.

Examples

The following example displays the FTP application's PAM information:

```
Router# show ipv6 port-map ftp
```

The following example displays PAM information at port number 21:

```
Router# show ipv6 port-map port 21
```

Related Commands

Command	Description
ipv6 port-map	Establishes PAM for the system.

show ipv6 prefix-list

To display information about an IPv6 prefix list or IPv6 prefix list entries, use the **show ipv6 prefix-list** command in user EXEC or privileged EXEC mode.

show ipv6 prefix-list [**detail | summary**] [*list-name*]

show ipv6 prefix-list *list-name ipv6-prefix/prefix-length* [**longer | first-match**]

show ipv6 prefix-list *list-name* **seq** *seq-num*

Syntax Description

detail | summary	(Optional) Displays detailed or summarized information about all IPv6 prefix lists.
list-name	(Optional) The name of a specific IPv6 prefix list.
ipv6-prefix	All prefix list entries for the specified IPv6 network. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/prefix-length	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
longer	(Optional) Displays all entries of an IPv6 prefix list that are more specific than the given *ipv6-prefix/prefix-length* values.
first-match	(Optional) Displays the entry of an IPv6 prefix list that matches the given *ipv6-prefix/prefix-length* values.
seq *seq-num*	The sequence number of the IPv6 prefix list entry.

Command Default

Displays information about all IPv6 prefix lists.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(2)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 Release 12.2(14)S.
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.
12.2(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 ipv6 prefix-list** command provides output similar to the **show ip prefix-list** command, except that it is IPv6-specific.

Examples

The following example shows the output of the **show ipv6 prefix-list** command with the **detail** keyword:

```
Router# show ipv6 prefix-list detail

Prefix-list with the last deletion/insertion: bgp-in
ipv6 prefix-list 6to4:
   count: 1, range entries: 0, sequences: 5 - 5, refcount: 2
   seq 5 permit 2002::/16 (hit count: 313, refcount: 1)
ipv6 prefix-list aggregate:
   count: 2, range entries: 2, sequences: 5 - 10, refcount: 30
   seq 5 deny 3FFE:C00::/24 ge 25 (hit count: 568, refcount: 1)
   seq 10 permit ::/0 le 48 (hit count: 31310, refcount: 1)
ipv6 prefix-list bgp-in:
   count: 6, range entries: 3, sequences: 5 - 30, refcount: 31
   seq 5 deny 5F00::/8 le 128 (hit count: 0, refcount: 1)
   seq 10 deny ::/0 (hit count: 0, refcount: 1)
   seq 15 deny ::/1 (hit count: 0, refcount: 1)
   seq 20 deny ::/2 (hit count: 0, refcount: 1)
   seq 25 deny ::/3 ge 4 (hit count: 0, refcount: 1)
   seq 30 permit ::/0 le 128 (hit count: 240664, refcount: 0)
```

Table 255 describes the significant fields shown in the display.

Table 255 show ipv6 prefix-list Field Descriptions

Field	Description
Prefix list with the latest deletion/insertion:	Prefix list that was last modified.
count	Number of entries in the list.
range entries	Number of entries with matching range.
sequences	Sequence number for the prefix entry.
refcount	Number of objects currently using this prefix list.
seq	Entry number in the list.
permit, deny	Granting status.
hit count	Number of matches for the prefix entry.

The following example shows the output of the **show ipv6 prefix-list** command with the **summary** keyword:

```
Router# show ipv6 prefix-list summary

Prefix-list with the last deletion/insertion: bgp-in
ipv6 prefix-list 6to4:
   count: 1, range entries: 0, sequences: 5 - 5, refcount: 2
ipv6 prefix-list aggregate:
   count: 2, range entries: 2, sequences: 5 - 10, refcount: 30
ipv6 prefix-list bgp-in:
   count: 6, range entries: 3, sequences: 5 - 30, refcount: 31
```

Related Commands

Command	Description
clear ipv6 prefix-list	Resets the hit count of the prefix list entries.
distribute-list in	Filters networks received in updates.
distribute-list out	Suppresses networks from being advertised in updates.
ipv6 prefix-list	Creates an entry in an IPv6 prefix list.
ipv6 prefix-list description	Adds a text description of an IPv6 prefix list.
match ipv6 address	Distributes IPv6 routes that have a prefix permitted by a prefix list.
neighbor prefix-list	Distributes BGP neighbor information as specified in a prefix list.
remark (prefix-list)	Adds a comment for an entry in a prefix list.

show ipv6 protocols

To display the parameters and current state of the active IPv6 routing protocol processes, use the **show ipv6 protocols** command in user EXEC or privileged EXEC mode.

show ipv6 protocols [**summary**]

Syntax Description

summary	(Optional) Displays the configured routing protocol process names.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(8)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 Release 12.2(14)S.
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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(15)T	The command output was modified to provide EIGRP information, including the vector metric.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.4	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The information displayed by the **show ipv6 protocols** command is useful in debugging routing operations.

Examples

The following is sample output from the **show ipv6 protocols** command, showing Intermediate System-to-Intermediate System (IS-IS) routing protocol information:

```
Router# show ipv6 protocols

IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "static"
IPv6 Routing Protocol is "isis"
  Interfaces:
    Ethernet0/0/3
    Ethernet0/0/1
    Serial1/0/1
    Loopback1 (Passive)
    Loopback2 (Passive)
    Loopback3 (Passive)
    Loopback4 (Passive)
```

```
    Loopback5 (Passive)
  Redistribution:
    Redistributing protocol static at level 1
  Inter-area redistribution
    Redistributing L1 into L2 using prefix-list word
  Address Summarization:
    L2: 33::/16  advertised with metric 0
    L2: 44::/16  advertised with metric 20
    L2: 66::/16  advertised with metric 10
    L2: 77::/16  advertised with metric 10
```

Table 256 describes the significant fields shown in the display.

Table 256 show ipv6 protocols Field Descriptions for IS-IS Processes

Field	Description
IPv6 Routing Protocol is	Specifies the IPv6 routing protocol used.
Interfaces	Specifies the interfaces on which the IPv6 IS-IS protocol is configured.
Redistribution	Lists the protocol that is being redistributed.
Inter-area redistribution	Lists the IS-IS levels that are being redistributed into other levels.
using prefix-list	Names the prefix list used in the interarea redistribution.
Address Summarization	Lists all the summary prefixes. If the summary prefix is being advertised then "advertised with metric *x*" will be displayed after the prefix.

The following is sample output from the **show ipv6 protocols** command, showing Border Gateway Protocol (BGP) routing protocol information for autonomous system 30:

```
Router# show ipv6 protocols

IPv6 Routing Protocol is "bgp 30"
  IGP synchronization is disabled
  Redistribution:
    Redistributing protocol connected
  Neighbor(s):
    Address                    FiltIn FiltOut Weight RoutemapIn RoutemapOut
    2002:3000::36C                  5       7    200
    5000::1                                           rmap-in    rmap-out
    7000::36C                                         rmap-in    rmap-out
```

Table 257 describes the significant fields shown in the display.

Table 257 show ipv6 protocols Field Descriptions for BGP Process

Field	Description
IPv6 Routing Protocol is	Specifies the IPv6 routing protocol used.
Redistribution	Lists the protocol that is being redistributed.
Address	Neighbor IPv6 address.
FiltIn	AS-path filter list applied to input.
FiltOut	AS-path filter list applied to output.

Table 257 show ipv6 protocols Field Descriptions for BGP Process (continued)

Field	Description
Weight	Neighbor weight value used in BGP bestpath selection.
RoutemapIn	Neighbor route map applied to input.
RoutemapOut	Neighbor route map applied to output.

The following is sample output from the **show ipv6 protocols** command with the **summary** keyword:

```
Router# show ipv6 protocols summary

Index Process Name
0     connected
1     static
2     rip myrip
3     bgp 30
```

The following is sample output from the **show ipv6 protocols** command and displays EIGRP information including the vector metric:

```
Router# show ipv6 protocols summary

IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "eigrp 1"
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Interfaces:
  Redistribution:
    Redistributing protocol eigrp 2 with metric 1 2 3 4 5
  Maximum path: 16
  Distance: internal 90 external 170

IPv6 Routing Protocol is "eigrp 2"
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Interfaces:
  Redistribution:
    None
  Maximum path: 16
  Distance: internal 90 external 170
```

show ipv6 rip

To display information about current IPv6 Routing Information Protocol (RIP) processes, use the **show ipv6 rip** command in user EXEC or privileged EXEC mode.

show ipv6 rip [*name*] [**database** | **next-hops**]

Syntax Description

name	(Optional) Name of the RIP process. If the name is not entered, details of all configured RIP processes will be displayed.
database	(Optional) Details of the entries in the specified RIP IPv6 routing table are displayed.
next-hops	(Optional) Details of the specified RIP IPv6 processes next hop addresses are displayed. If no RIP process name is specified, the next hop addresses for all RIP IPv6 processes will be displayed.

Command Default

Information about all current IPv6 RIP processes is displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(2)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 12.2(22)S, and the *name* argument and the **database** and **next-hops** keywords were added.
12.2(13)T	The modifications to add the *name* argument and the **database** and **next-hops** keywords were added.
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.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
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 introduced on Cisco ASR 1000 Series Routers.

Examples

The following is sample output from the **show ipv6 rip** command:

```
Router# show ipv6 rip

RIP process "one", port 521, multicast-group FF02::9, pid 55
     Administrative distance is 25. Maximum paths is 4
     Updates every 30 seconds, expire after 180
     Holddown lasts 0 seconds, garbage collect after 120
```

```
     Split horizon is on; poison reverse is off
     Default routes are not generated
     Periodic updates 8883, trigger updates 2
  Interfaces:
    Ethernet2
  Redistribution:
RIP process "two", port 521, multicast-group FF02::9, pid 61
     Administrative distance is 120. Maximum paths is 4
     Updates every 30 seconds, expire after 180
     Holddown lasts 0 seconds, garbage collect after 120
     Split horizon is on; poison reverse is off
     Default routes are not generated
     Periodic updates 8883, trigger updates 0
  Interfaces:
    None
  Redistribution:
```

Table 258 describes the significant fields shown in the display.

Table 258 show ipv6 rip Field Descriptions

Field	Description
RIP process	The name of the RIP process.
port	The port that the RIP process is using.
multicast-group	The IPv6 multicast group of which the RIP process is a member.
pid	The process identification number (pid) assigned to the RIP process.
Administrative distance	Used to rank the preference of sources of routing information. Connected routes have an administrative distance of 1 and are preferred over the same route learned by a protocol with a larger administrative distance value.
Updates	The value (in seconds) of the update timer.
expire	The interval (in seconds) in which updates expire.
Holddown	The value (in seconds) of the hold-down timer.
garbage collect	The value (in seconds) of the garbage-collect timer.
Split horizon	The split horizon state is either on or off.
poison reverse	The poison reverse state is either on or off.
Default routes	The origination of a default route into RIP. Default routes are either generated or not generated.
Periodic updates	The number of RIP update packets sent on an update timer.
trigger updates	The number of RIP update packets sent as triggered updates.

To display information about a specified IPv6 RIP process database, enter the **show ipv6 rip** command with the *name* argument and the **database** keyword. In the following output for the IPv6 RIP process named one, timer information is displayed, and route 3004::/64 has a route tag set:

```
Router# show ipv6 rip one database

RIP process "one", local RIB
 2001:72D:1000::/64, metric 2
     Ethernet2/FE80::202:7DFF:FE1A:9472, expires in 168 secs
 2001:72D:2000::/64, metric 2, installed
     Ethernet2/FE80::202:7DFF:FE1A:9472, expires in 168 secs
 2001:72D:3000::/64, metric 2, installed
```

```
    Ethernet2/FE80::202:7DFF:FE1A:9472, expires in 168 secs
    Ethernet1/FE80::203:7EBC:FE23:1000, expires in 120 secs
2001:72D:4000::/64, metric 16, expired, [advertise 119/hold 0]
    Ethernet2/FE80::202:7DFF:FE1A:9472
3004::/64, metric 2 tag 2A, installed
    Ethernet2/FE80::202:7DFF:FE1A:9472, expires in 168 secs
```

Table 259 describes the significant fields shown in the display.

Table 259 show ipv6 rip database Field Descriptions

Field	Description
RIP process	The name of the RIP process.
2001:72D:1000::/64	The IPv6 route prefix.
metric	Metric for the route.
installed	Route is installed in the IPv6 routing table.
Ethernet2/FE80::202:7DFF:FE1A:9472	Interface and LL next hop through which the IPv6 route was learned.
expires in	The interval (in seconds) before the route expires.
advertise	For an expired route, the value (in seconds) during which the route will be advertised as expired.
hold	The value (in seconds) of the hold-down timer.
tag	Route tag.

To display information about the next-hops for a specified IPv6 RIP process, enter the **show ipv6 rip** command with the *name* argument and the **next-hops** keyword:

```
Router# show ipv6 rip one next-hops

RIP process "one", Next Hops
  FE80::210:7BFF:FEC2:ACCF/Ethernet4/2 [1 routes]
  FE80::210:7BFF:FEC2:B286/Ethernet4/2 [2 routes]
```

Table 260 describes the significant fields shown in the display.

Table 260 show ipv6 rip next-hops Field Descriptions

Field	Description
RIP process	The name of the RIP process.
FE80::210:7BFF:FEC2:ACCF/Ethernet4/2	The next hop address and interface through which it was learned. Next hops are either the addresses of IPv6 RIP neighbors from which we have learned routes, or explicit next hops received in IPv6 RIP advertisements. **Note** An IPv6 RIP neighbor may choose to advertise all its routes with an explicit next hop. In this case the address of the neighbor would not appear in the next hop display.
[1 routes]	The number of routes in the IPv6 RIP routing table using the specified next hop.

show ipv6 route

To display the current contents of the IPv6 routing table, use the **show ipv6 route** command in user EXEC or privileged EXEC mode.

show ipv6 route [*ipv6-address* | *ipv6-prefix*/*prefix-length* [**longer-prefixes**] | [*protocol*] [**updated** [**boot-up**] [*day month*] [*time*]] | **interface** *interface-type interface-number* | **nsf** | **table** *table-id* | **watch**]

Syntax Description

ipv6-address	(Optional) Displays routing information for a specific IPv6 address. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal format using 16-bit values between colons.
ipv6-prefix	(Optional) Displays routing information for a specific IPv6 network. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal format using 16-bit values between colons.
/prefix-length	(Optional) The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
longer-prefixes	(Optional) Displays output for longer prefix entries.
protocol	(Optional) Displays routes for the specified routing protocol using any of these keywords: **bgp**, **isis**, **eigrp**, **ospf**, or **rip** or displays routes for the specified type of route using any of these keywords: **connected**, **local**, **mobile**, or **static**.
updated	(Optional) Displays routes with time stamps.
boot-up	(Optional) Displays routing information since the boot up.
day month	(Optional) Displays routes since the day and month specified.
time	(Optional) Displays routes since the time specified. The time is specified in *hh:mm* format.
interface *interface-type*	(Optional) Interface type. For more information about supported interface types, use the question mark (?) online help function.
interface-number	(Optional) Interface number. For more information about the numbering syntax for supported interface types, use the question mark (?) online help function.
nsf	(Optional) Displays routes in the nonstop forwarding state.
table *table-id*	(Optional) Displays IPv6 Routing Information Base (RIB) table information for the specified table ID. The table must be in a hexadecimal format. Range for table ID is 0 to 0-0xFFFFFFFF.
watch	(Optional) Displays information on route watchers.

Command Default All IPv6 routing information for all active routing tables is displayed.

Command Modes
User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(8)T	This command was modified. The **isis** protocol keyword was added to the command syntax, and the I1 - ISIS L1, I2 - ISIS L2, and IA - ISIS interarea fields were added to the command output.
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, the timer information was removed, and an indicator was added to display IPv6 MPLS virtual interfaces.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T, the timer information was removed, and an indicator was added to display IPv6 MPLS virtual interfaces.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S. The **longer-prefixes** keyword was 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.
12.2(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 introduced on Cisco ASR 1000 series routers.
12.4(24)T	This command was modified in a release earlier than Cisco IOS Release 12.4(24)T. The **table**, **nsf**, **watch**, and **updated** keywords and *day, month, table-id*, and *time* arguments were added.

Usage Guidelines The **show ipv6 route** command provides output similar to the **show ip route** command, except that the information is IPv6-specific.

When the *ipv6-address* or *ipv6-prefix/prefix-length* argument is specified, a longest match lookup is performed from the routing table and only route information for that address or network is displayed. When a routing protocol is specified, only routes for that protocol are displayed. When the **connected**, **local**, **mobile**, or **static** keyword is specified, only that type of route is displayed. When the *interface-type interface-number* arguments are specified, only the specified interface-specific routes are displayed.

Examples

show ipv6 route Command with No Keyword Specified Example

The following is sample output from the **show ipv6 route** command when entered without an IPv6 address or prefix specified:

```
Router# show ipv6 route
```

```
IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       I1 - ISIS L1, I2 - ISIS L2, IA - IIS interarea
B   3000::/64 [20/0]
     via FE80::A8BB:CCFF:FE02:8B00, Serial6/0
L   4000::2/128 [0/0]
     via ::, Ethernet1/0
C   4000::/64 [0/0]
     via ::, Ethernet1/0
LC  4001::1/128 [0/0]
     via ::, Loopback0
L   5000::2/128 [0/0]
     via ::, Serial6/0
C   5000::/64 [0/0]
     via ::, Serial6/0
S   5432::/48 [1/0]
     via 4000::1, Null
L   FE80::/10 [0/0]
     via ::, Null0
L   FF00::/8 [0/0]
     via ::, Null0
```

Table 261 describes the significant fields shown in the display.

Table 261 show ipv6 route Field Descriptions

Field	Description
Codes:	Indicates the protocol that derived the route. Values are as follows: • C—Connected • L—Local • S—Static • R—RIP derived • B—BGP derived • I1—ISIS L1—Integrated IS-IS Level 1 derived • I2—ISIS L2—Integrated IS-IS Level 2 derived • IA—ISIS interarea—Integrated IS-IS interarea derived
2001:0DB8:DDDD::/32	Indicates the IPv6 prefix of the remote network.
[200/0]	The first number in the brackets is the administrative distance of the information source; the second number is the metric for the route.
via ::FFFF:192.168.99.70	Specifies the address of the next router to the remote network.
IPv6-mpls	Specifies the interface through which the next router to the specified network can be reached. **Note** In this example output, the interface is the IPv6 Multiprotocol Label Switching (MPLS) virtual interface used in the 6PE feature where IPv6 traffic is sent across an IPv4 MPLS backbone from one IPv6 provider edge router to another.

show ipv6 route Command with Address or Prefix Specified Example

When the *ipv6-address* or *ipv6-prefix/prefix-length* argument is specified, only route information for that address or network is displayed. The following is sample output from the **show ipv6 route** command when entered with the IPv6 prefix 2001:200::/35:

```
Router# show ipv6 route 2001:200::/35

IPv6 Routing Table - 261 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea

B 2001:200::/35 [20/3]
  via FE80::60:5C59:9E00:16, Tunnel1
```

show ipv6 route Command with Protocol Specified Example

When you specify a protocol, only routes for that particular routing protocol are shown. The following is sample output from the **show ipv6 route** command when entered with the **bgp** keyword:

```
Router# show ipv6 route bgp

IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
B   3000::/64 [20/0]
     via FE80::A8BB:CCFF:FE02:8B00, Serial6/0
```

show ipv6 route Command for Local Routes Example

The following is sample output from the **show ipv6 route** command when entered with the **local** router address:

```
Router# show ipv6 route local

IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
L   4000::2/128 [0/0]
     via ::, Ethernet1/0
LC  4001::1/128 [0/0]
     via ::, Loopback0
L   5000::2/128 [0/0]
     via ::, Serial6/0
L   FE80::/10 [0/0]
     via ::, Null0
L   FF00::/8 [0/0]
     via ::, Null0
```

show ipv6 route Command for 6PE Multipath Example'

The following is sample output from the **show ipv6 route** command when used with the 6PE multipath feature enabled:

```
Router# show ipv6 route

IPv6 Routing Table - default - 19 entries
Codes:C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
.
.
.
B   4004::/64 [200/0]
```

```
via ::FFFF:172.11.11.1
via ::FFFF:172.30.30.1
```

Related Commands

Command	Description
ipv6 route	Establishes a static IPv6 route.
show ipv6 interface	Displays IPv6 interface information.
show ipv6 route summary	Displays the current contents of the IPv6 routing table in summary format.
show ipv6 tunnel	Displays IPv6 tunnel information.

show ipv6 route shortcut

To display the IPv6 routes that contain shortcuts, use the **show ipv6 route shortcut** command in privileged EXEC mode.

show ipv6 route shortcut

Syntax Description

This command has no arguments or keywords.

Command Default

IPv6 information about shortcuts for all active routing tables is displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)S	This command was introduced.

Usage Guidelines

The **show ipv6 route shortcut** command displays only the routes that have overriding shortcut paths.

Examples

The following is sample output from the **show ipv6 route shortcut** command:

```
Router# show ipv6 route shortcut

IPv6 Routing Table - default - 7 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO
       ND - Neighbor Discovery, l - LISP
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
S 7000:1::/64 [1/0]
    via 4000:1:1::1, Ethernet1/1 [Shortcut]
    via 5000:1:1::1, Ethernet1/1 [Shortcut]
    via Ethernet1/1, directly connected
S 8000:1:1::/64 [1/0]
    via 6000:1:1::1, Ethernet0/1 [Shortcut]
    via Ethernet0/0, directly connected
```

Table 261 describes the significant fields shown in the display.

Table 262 show ipv6 route shortcut Field Descriptions

Field	Description
Codes:	Indicates the protocol that derived the route. Values are as follows: • C—Connected • L—Local • S—Static • R—RIP derived • B—BGP derived • I1—ISIS L1—Integrated IS-IS Level 1 derived • I2—ISIS L2—Integrated IS-IS Level 2 derived • IA—ISIS interarea—Integrated IS-IS interarea derived
S 7000:1::/64 [1/0]	Indicates paths that may be shortcut paths.
via 4000:1:1::1, Ethernet1/1	Indicates a path that may be a shortcut path.
via 5000:1:1::1, Ethernet1/1 [Shortcut]	Indicates a path that may be a shortcut path.
via Ethernet1/1, directly connected	Shows routes connected to the router directly.

Related Commands

Command	Description
ipv6 route	Establishes a static IPv6 route.
show ipv6 interface	Displays IPv6 interface information.
show ipv6 route summary	Displays the current contents of the IPv6 routing table in summary format.
show ipv6 tunnel	Displays IPv6 tunnel information.

show ipv6 route summary

To display the current contents of the IPv6 routing table in summary format, use the **show ipv6 route summary** command in user EXEC or privileged EXEC mode.

show ipv6 route summary

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(2)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 Release 12.2(14)S.
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.
12.2(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 ipv6 route summary** command:

```
Router# show ipv6 route summary

IPv6 Routing Table Summary - 257 entries
  37 local, 35 connected, 25 static, 0 RIP, 160 BGP
  Number of prefixes:
    /16: 1, /24: 46, /28: 10, /32: 5, /35: 25, /40: 1, /48: 63, /64: 19
    /96: 15, /112: 1, /126: 31, /127: 4, /128: 36
```

Table 263 describes the significant fields shown in the display.

Table 263 show ipv6 route summary Field Descriptions

Field	Description
entries	Number of entries in the IPv6 routing table.
Route source	Number of routes that are present in the routing table for each route source, which can be local routes, connected routes, static routes, a routing protocol, prefix and address or name, and longer prefixes and address or name. Routing protocols can include RIP, IS-IS, OSPF, and BGP. Other route sources can be connected, local, static, or a specific interface.
Number of prefixes:	Number of routing table entries for given prefix length.

Related Commands

Command	Description
show ipv6 route	Displays the current contents of the IPv6 routing table.

show ipv6 route vrf

To display the IPv6 routing table associated with a Virtual Private Network (VPN) routing and forwarding (VRF) instance, use the **show ipv6 route vrf** command in user EXEC or privileged EXEC mode.

show ipv6 route vrf {*vrf-name* | *vrf-number*}

Syntax Description

vrf-name	Name assigned to the VRF.
vrf-number	Hexadecimal number assigned to the VRF.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.2(33)SRB1	This command was integrated into Cisco IOS Release 12.2(33)SRB1.
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.

Usage Guidelines

The **show ipv6 route vrf** command displays specified information from the IPv6 routing table of a VRF.

Examples

The following is sample output regarding an IPv6 routing table associated with a VRF named cisco1:

```
Router# show ipv6 route vrf cisco1

IPv6 Routing Table cisco1 - 6 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
C   2001:8::/64 [0/0]
     via ::, FastEthernet0/0
L   2001:8::3/128 [0/0]
     via ::, FastEthernet0/0
B   2002:8::/64 [200/0]
     via ::FFFF:192.168.1.4,
B   2010::/64 [20/1]
     via 2001:8::1,
C   2012::/64 [0/0]
     via ::, Loopback1
L   2012::1/128 [0/0]
     via ::, Loopback1
```

Table 264 describes the significant fields shown in the display.

Table 264 show ipv6 route vrf Field Descriptions

Field	Description
2001:8::/64 [0/0]	Network number.
via ::, FastEthernet0/0	Indicates how the route was derived.

show ipv6 routers

To display IPv6 router advertisement information received from onlink routers, use the **show ipv6 routers** command in user EXEC or privileged EXEC mode.

show ipv6 routers [*interface-type interface-number*] [**conflicts**]

Syntax Description

interface-type	(Optional) Specifies the interface type.
interface-number	(Optional) Specifies the interface number.
conflicts	(Optional) Displays router advertisements that differ from the advertisements configured for a specified interface.

Command Default

When an interface is not specified, onlink router advertisement information is displayed for all interface types. (The term *onlink* refers to a locally reachable address on the link.)

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(2)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 Release 12.2(14)S.
12.4(2)T	Command output was updated to show the state of the default router preference (DRP) preference value as advertised by other routers.
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.
12.2(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

Routers advertising parameters that differ from the advertisement parameters configured for the interface on which the advertisements are received are marked as conflicting.

Examples

The following is sample output from the **show ipv6 routers** command when entered without an IPv6 interface type and number:

```
Router# show ipv6 routers

Router FE80::83B3:60A4 on Tunnel5, last update 3 min
  Hops 0, Lifetime 6000 sec, AddrFlag=0, OtherFlag=0
  Reachable time 0 msec, Retransmit time 0 msec
  Prefix 3FFE:C00:8007::800:207C:4E37/96 autoconfig
```

```
    Valid lifetime -1, preferred lifetime -1
Router FE80::290:27FF:FE8C:B709 on Tunnel57, last update 0 min
  Hops 64, Lifetime 1800 sec, AddrFlag=0, OtherFlag=0
  Reachable time 0 msec, Retransmit time 0 msec
```

The following sample output shows a single neighboring router that is advertising a high default router preference and is indicating that it is functioning as a Mobile IPv6 home agent on this link.

```
Router# show ipv6 routers

Router FE80::100 on Ethernet0/0, last update 0 min
  Hops 64, Lifetime 50 sec, AddrFlag=0, OtherFlag=0, MTU=1500
  HomeAgentFlag=1, Preference=High
  Reachable time 0 msec, Retransmit time 0 msec
  Prefix 2001::100/64 onlink autoconfig
    Valid lifetime 2592000, preferred lifetime 604800
```

Table 265 describes the significant fields shown in the previous two displays.

Table 265 show ipv6 routers Field Descriptions

Field	Description
Hops	The configured hop limit value for the router advertisement.
Lifetime	The configured Router Lifetime value for the router advertisement. A value of 0 indicates that the router is not a default router. A value other than 0 indicates that the router is a default router.
AddrFlag	If the value is 0, the router advertisement received from the router indicates that addresses are not configured using the stateful autoconfiguration mechanism. If the value is 1, the addresses are configured using this mechanism.
OtherFlag	If the value is 0, the router advertisement received from the router indicates that information other than addresses is not obtained using the stateful autoconfiguration mechanism. If the value is 1, other information is obtained using this mechanism. (The value of OtherFlag can be 1 only if the value of AddrFlag is 1.)
MTU	The maximum transmission unit (MTU).
HomeAgentFlag=1	The value can be either 0 or 1. A value of 1 indicates that the router from which the RouterAdvertisement was received is functioning as a Mobile IPv6 home agent on this link, and a value of 0 indicates it is not functioning as a Mobile IPv6 home agent on this link.
Preference=High	The default router preference. The value can be high, medium, or low.
Retransmit time	The configured RetransTimer value. The time value to be used on this link for neighbor solicitation transmissions, which are used in address resolution and neighbor unreachability detection. A value of 0 means the time value is not specified by the advertising router.
Prefix	A prefix advertised by the router. Also indicates if onlink or autoconfig bits were set in the router advertisement message.
Valid lifetime	The length of time (in seconds) relative to the time the advertisement is sent that the prefix is valid for the purpose of onlink determination. A value of –1 (all ones, 0xffffffff) represents infinity.
preferred lifetime	The length of time (in seconds) relative to the time the advertisements is sent that addresses generated from the prefix via address autoconfiguration remain valid. A value of –1 (all ones, 0xffffffff) represents infinity.

When the *interface-type* and *interface-number* arguments are specified, router advertisement details about that specific interface are displayed. The following is sample output from the **show ipv6 routers** command when entered with an interface type and number:

```
Router# show ipv6 routers tunnel 5

Router FE80::83B3:60A4 on Tunnel5, last update 5 min
  Hops 0, Lifetime 6000 sec, AddrFlag=0, OtherFlag=0
  Reachable time 0 msec, Retransmit time 0 msec
  Prefix 3FFE:C00:8007::800:207C:4E37/96 autoconfig
    Valid lifetime -1, preferred lifetime -1
```

Entering the **conflicts** keyword with the **show ipv6 routers** command displays information for routers that are advertising parameters different from the parameters configured for the interface on which the advertisements are being received, as the following sample output shows:

```
Router# show ipv6 routers conflicts

Router FE80::203:FDFF:FE34:7039 on Ethernet1, last update 1 min, CONFLICT
   Hops 64, Lifetime 1800 sec, AddrFlag=0, OtherFlag=0
   Reachable time 0 msec, Retransmit time 0 msec
   Prefix 2003::/64 onlink autoconfig
     Valid lifetime -1, preferred lifetime -1
Router FE80::201:42FF:FECA:A5C on Ethernet1, last update 0 min, CONFLICT
   Hops 64, Lifetime 1800 sec, AddrFlag=0, OtherFlag=0
   Reachable time 0 msec, Retransmit time 0 msec
   Prefix 2001::/64 onlink autoconfig
     Valid lifetime -1, preferred lifetime -1
```

show ipv6 rpf

To check Reverse Path Forwarding (RPF) information for a given unicast host address and prefix, use the **show ipv6 rpf** command in user EXEC or privileged EXEC mode.

show ipv6 rpf [**vrf** *vrf-name*] *ipv6-prefix*

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
ipv6-prefix	Summary prefix designated for a range of IPv6 prefixes. The *ipv6-prefix* argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)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 introduced on Cisco ASR 1000 Series Routers.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

The **show ipv6 rpf** command displays how IPv6 multicast routing performs RPF. Because the router can find RPF information from multiple routing tables (for example, unicast Routing Information Base [RIB], multiprotocol Border Gateway Protocol [BGP] routing table, or static mroutes), the **show ipv6 rpf** command displays the source from which the information is retrieved.

Examples

The following example displays RPF information for the unicast host with the IPv6 address of 2001::1:1:2:

```
Router# show ipv6 rpf 2001::1:1:2

RPF information for 2001::1:1:2
  RPF interface:Ethernet3/2
  RPF neighbor:FE80::40:1:3
  RPF route/mask:20::/64
  RPF type:Unicast
  RPF recursion count:0
  Metric preference:110
```

```
Metric:30
```

Table 266 describes the significant fields shown in the display.

Table 266 show ipv6 rpf Field Descriptions

Field	Description
RPF information for 2001::1:1:2	Source address that this information concerns.
RPF interface:Ethernet3/2	For the given source, the interface from which the router expects to get packets.
RPF neighbor:FE80::40:1:3	For the given source, the neighbor from which the router expects to get packets.
RPF route/mask:20::/64	Route number and mask that matched against this source.
RPF type:Unicast	Routing table from which this route was obtained, either unicast, multiprotocol BGP, or static mroutes.
RPF recursion count	Indicates the number of times the route is recursively resolved.
Metric preference:110	The preference value used for selecting the unicast routing metric to the Route Processor (RP) announced by the designated forwarder (DF).
Metric:30	Unicast routing metric to the RP announced by the DF.

show ipv6 snooping capture-policy

To display message capture policies, use the **show ipv6 snooping capture-policy** command in user EXEC or privileged EXEC mode.

show ipv6 snooping capture-policy [**interface** *type number*]

Syntax Description

interface *type number*	(Optional) Displays first-hop message types on the specified interface type and number.

Command Modes

User EXEC
Privileged EXEC (#)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

The **show ipv6 snooping capture-policy** command displays IPv6 first-hop message capture policies.

Examples

The following example shows **show ipv6 snooping capture-policy** command output on the Ethernet 0/0 interface, on which the IPv6 Neighbor Discovery Protocol (NDP) inspection and Router Advertisement (RA) Guard features are configured:

```
Router# show ipv6 snooping capture-policy

Hardware policy registered on Et0/0
Protocol  Protocol value  Message  Value  Action  Feature
ICMP      58              RS       85     punt    RA Guard
                                          punt    ND Inspection
ICMP      58              RA       86     drop    RA guard
                                          punt    ND Inspection
ICMP      58              NS       87     punt    ND Inspection
ICMP      58              NA       88     punt    ND Inspection
ICMP      58              REDIR    89     drop    RA Guard
                                          punt    ND Inspection
```

Table 267 describes the significant fields shown in the display.

Table 267 show ipv6 snooping capture-policy Field Descriptions

Field	Description
Hardware policy registered on Fa4/11	A hardware policy contains a programmatic access list (ACL), with a list of access control entries (ACEs).
Protocol	The protocol whose packets are being inspected.
Message	The type of message being inspected.

Table 267 show ipv6 snooping capture-policy Field Descriptions (continued)

Field	Description
Action	Action to be taken on the packet.
Feature	The inspection feature for this information.

show ipv6 snooping counters

To display information about the packets counted by the interface counter, use the **show ipv6 snooping counters** command in user EXEC or privileged EXEC mode.

show ipv6 snooping counters [**interface** *type number*]

Syntax Description

interface *type number*	(Optional) Displays first hop packets that match the specified interface type and number.

Command Modes

User EXEC
Privileged EXEC (#)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

The **show ipv6 snooping counters** command shows packets handled by the switcher that are being counted in interface counters. The switcher counts packets captured per interface and records whether the packet was received, sent, or dropped. If a packet is dropped, the reason for the drop and the feature that caused the drop are both also provided.

Examples

The following examples shows information about packets counted on interface FastEthernet4/12:

```
Router# show ipv6 snooping counters interface Fa4/12

Received messages on Fa4/12:
Protocol        Protocol message
ICMPv6          RS      RA      NS      NA      REDIR   CPS     CPA
                0       4256    0       0       0       0       0

Bridged messages from Fa4/12:
Protocol        Protocol message
ICMPv6          RS      RA      NS      NA      REDIR   CPS     CPA
                0       4240    0       0       0       0       0

Dropped messages on Fa4/12:
Feature/Message RS      RA      NS      NA      REDIR   CPS     CPA
RA guard        0       16      0       0       0       0       0

Dropped reasons on Fa4/12:
RA guard         16   RA drop - reason:RA/REDIR received on un-authorized port
```

Table 267 describes the significant fields shown in the display.

Table 268 show ipv6 snooping counters Field Descriptions

Field	Description
Received messages on Fa4/12:	The messages received on an interface.
Protocol	The protocol for which messages are being counted.
Protocol message	The type of protocol messages being counted.
Bridged messages from Fa4/12:	Bridged messages from the interface.
Dropped messages an Fa4/12:	The messages dropped on the interface.
Feature/message	The feature that caused the drop, and the type and number of messages dropped.
RA drop - reason:RA/REDIR received on un-authorized port	The reason these messages were dropped.

show ipv6 snooping features

To display information about about snooping features configured on the router, use the **show ipv6 snooping features** command in user EXEC or privileged EXEC mode.

show ipv6 snooping features

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC (#)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

The **show ipv6 snooping features** command shows the first hop features that are configured on the router.

Examples

The following example shows that both IPv6 ND inspection and IPv6 RA Guard are configured on the router:

```
Router# show ipv6 snooping features

Feature name   priority state
RA guard          100   READY
NDP inspection     20   READY
```

Table 267 describes the significant fields shown in the display.

Table 269 show ipv6 snooping features Field Descriptions

Field	Description
Feature name	The names of the IPv6 global policy features configured on the router.
Priority	The priority of the specified feature.
State	The state of the specified feature.

show ipv6 snooping policies

To display information about the configured policies and the interfaces to which they are attached, use the **show ipv6 snooping policies** command in user EXEC or privileged EXEC mode.

show ipv6 snooping policies [**interface** *type number*]

Syntax Description

interface *type number*	(Optional) Displays policies that match the specified interface type and number.

Command Modes

User EXEC
Privileged EXEC (#)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

The **show ipv6 snooping policies** command displaying all policies that are configured, and lists the interfaces to which they are attached.

Examples

The following examples shows information about all policies configured:

```
Router# show ipv6 snooping policies

NDP inspection policies configured:

Policy      Interface    Vlan
------      ---------    ----
trusted      Et0/0        all
             Et1/0        all
untrusted    Et2/0        all

RA guard policies configured:

Policy      Interface    Vlan
------      ---------    ----
host         Et0/0        all
             Et1/0        all
router       Et2/0        all
```

Table 267 describes the significant fields shown in the display..

Table 270 show ipv6 first-hop policies Field Descriptions

Field	Description
NDP inspection policies configured:	Description of the policies configured for a specific feature.
Policy	Whether the policy is trusted or untrusted.
Interface	The interface to which a policy is attached.

show ipv6 spd

To display the IPv6 Selective Packet Discard (SPD) configuration, use the **show ipv6 spd** command in privileged EXEC mode.

show ipv6 spd

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T.

Usage Guidelines

Use the **show ipv6 spd** command to display the SPD configuration, which may provide useful troubleshooting information.

Examples

The following is sample output from the **show ipv6 spd** command:

```
Router# show ipv6 spd

Current mode: normal
Queue max threshold: 74, Headroom: 100, Extended Headroom: 10
IPv6 packet queue: 0
```

Table 267 describes the significant fields shown in the display.

Table 271 show ipv6 spd Field Description

Field	Description
Current mode: normal	The current SPD state or mode.
Queue max threshold: 74	The process input queue maximum.

Related Commands

Command	Description
ipv6 spd queue max-threshold	Configures the maximum number of packets in the SPD process input queue.

show ipv6 static

To display the current contents of the IPv6 routing table, use the **show ipv6 static** command in user EXEC or privileged EXEC mode.

show ipv6 static [*ipv6-address* | *ipv6-prefix*/*prefix-length*] [**interface** *type number* | **recursive**] [**detail**]

Syntax Description

ipv6-address	(Optional) Provides routing information for a specific IPv6 address. 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	(Optional) Provides routing information for a specific IPv6 network. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/prefix-length	(Optional) The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
interface	(Optional) Name of an interface.
type	(Optional, but required if the **interface** keyword is used) Interface type. For a list of supported interface types, use the question mark (?) online help function.
number	(Optional, but required if the **interface** keyword is used) Interface number. For specific numbering syntax for supported interface types, use the question mark (?) online help function.
recursive	(Optional) Allows the display of recursive static routes only.
detail	(Optional) Specifies the following additional information: • For valid recursive routes, the output path set and maximum resolution depth. • For invalid recursive routes, the reason why the route is not valid. • For invalid direct or fully specified routes, the reason why the route is not valid.

Command Default

All IPv6 routing information for all active routing tables is displayed.

Command Modes

User EXEC
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.

Release	Modification
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.
12.2(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 2.1.0	This command was modified. It was integrated into Cisco IOS XE Release 2.1.0.
15.1(2)T	This command was modified. Support for IPv6 was added to Cisco IOS Release 15.1(2)T.

Usage Guidelines

The **show ipv6 static** command provides output similar to the **show ip route** command, except that it is IPv6-specific.

When the *ipv6-address* or *ipv6-prefix*/*prefix-length* argument is specified, a longest match lookup is performed from the routing table and only route information for that address or network is displayed. Only the information matching the criteria specified in the command syntax is displayed. For example, when the *type number* arguments are specified, only the specified interface-specific routes are displayed.

Examples

show ipv6 static Command with No Options Specified in the Command Syntax Example

When no options specified in the command, those routes installed in the IPv6 Routing Information Base (RIB) are marked with an asterisk, as shown in the following example:

```
Router# show ipv6 static

IPv6 Static routes
Code: * - installed in RIB
* 3000::/16, interface Ethernet1/0, distance 1
* 4000::/16, via nexthop 2001:1::1, distance 1
  5000::/16, interface Ethernet3/0, distance 1
* 5555::/16, via nexthop 4000::1, distance 1
  5555::/16, via nexthop 9999::1, distance 1
* 5555::/16, interface Ethernet2/0, distance 1
* 6000::/16, via nexthop 2007::1, interface Ethernet1/0, distance 1
```

Table 272 describes the significant fields shown in the display.

Table 272 show ipv6 static Field Descriptions

Field	Description
via nexthop	Specifies the address of the next router in the path to the remote network.
distance 1	Indicates the administrative distance to the specified route.

show ipv6 static Command with the IPv6 Address and Prefix Example

When the *ipv6-address* or *ipv6-prefix*/*prefix-length* argument is specified, only information about static routes for that address or network is displayed. The following is sample output from the **show ipv6 route** command when entered with the IPv6 prefix 2001:200::/35:

```
Router# show ipv6 static 2001:200::/35
```

```
IPv6 Static routes
Code: * - installed in RIB
* 2001:200::/35, via nexthop 4000::1, distance 1
  2001:200::/35, via nexthop 9999::1, distance 1
* 2001:200::/35, interface Ethernet2/0, distance 1
```

show ipv6 static interface Command Example

When an interface is supplied, only those static routes with the specified interface as the outgoing interface are displayed. The **interface** keyword may be used with or without the IPv6 address and prefix specified in the command statement.

```
Router# show ipv6 static interface ethernet 3/0

IPv6 Static routes
Code: * - installed in RIB
  5000::/16, interface Ethernet3/0, distance 1
```

show ipv6 static recursive Command Example

When the **recursive** keyword is specified, only recursive static routes are displayed:

```
Router# show ipv6 static recursive

IPv6 Static routes
Code: * - installed in RIB
* 4000::/16, via nexthop 2001:1::1, distance 1
* 5555::/16, via nexthop 4000::1, distance 1
  5555::/16, via nexthop 9999::1, distance 1
```

show ipv6 static detail Command Example

When the **detail** keyword is specified, the following additional information is displayed:

- For valid recursive routes, the output path set and maximum resolution depth.
- For invalid recursive routes, the reason why the route is not valid.
- For invalid direct or fully specified routes, the reason why the route is not valid.

```
Router# show ipv6 static detail

IPv6 Static routes
Code: * - installed in RIB
* 3000::/16, interface Ethernet1/0, distance 1
* 4000::/16, via nexthop 2001:1::1, distance 1
     Resolves to 1 paths (max depth 1)
     via Ethernet1/0
  5000::/16, interface Ethernet3/0, distance 1
     Interface is down
* 5555::/16, via nexthop 4000::1, distance 1
     Resolves to 1 paths (max depth 2)
     via Ethernet1/0
  5555::/16, via nexthop 9999::1, distance 1
     Route does not fully resolve
* 5555::/16, interface Ethernet2/0, distance 1
* 6000::/16, via nexthop 2007::1, interface Ethernet1/0, distance 1
```

Related Commands

Command	Description
ipv6 route	Establishes a static IPv6 route.
show ip route	Displays the current state of the routing table.

Command	Description
show ipv6 interface	Displays IPv6 interface information.
show ipv6 route summary	Displays the current contents of the IPv6 routing table in summary format.
show ipv6 tunnel	Displays IPv6 tunnel information.

show ipv6 traffic

To display statistics about IPv6 traffic, use the **show ipv6 traffic** command in user EXEC or privileged EXEC mode.

show ipv6 traffic [**interface** [*interface type number*]]

Syntax Description

interface	(Optional) All interfaces. IPv6 forwarding statistics for all interfaces on which IPv6 forwarding statistics are being kept will be displayed.
interface type number	(Optional) Specified interface. Interface statistics that have occurred since the statistics were last cleared on the specific interface are displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(2)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, and output fields were added.
12.2(13)T	The modification to add output fields was integrated into this release.
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.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
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.
12.2(33)SRC	The *interface* argument and **interface** keyword were added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The **show ipv6 traffic** command provides output similar to the **show ip traffic** command, except that it is IPv6-specific.

Examples

The following is sample output from the **show ipv6 traffic** command:

```
Router# show ipv6 traffic

IPv6 statistics:
  Rcvd:  0 total, 0 local destination
         0 source-routed, 0 truncated
         0 format errors, 0 hop count exceeded
```

```
         0 bad header, 0 unknown option, 0 bad source
         0 unknown protocol, 0 not a router
         0 fragments, 0 total reassembled
         0 reassembly timeouts, 0 reassembly failures
         0 unicast RPF drop, 0 suppressed RPF drop
  Sent:  0 generated, 0 forwarded
         0 fragmented into 0 fragments, 0 failed
         0 encapsulation failed, 0 no route, 0 too big
  Mcast: 0 received, 0 sent

ICMP statistics:
  Rcvd: 0 input, 0 checksum errors, 0 too short
        0 unknown info type, 0 unknown error type
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 0 router advert, 0 redirects
```

The following is sample output for the **show ipv6 interface** command without IPv6 CEF running:

```
Router# show ipv6 interface ethernet 0/1/1

Ethernet0/1/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::203:FDFF:FE49:9
  Description: sat-2900a f0/12
  Global unicast address(es):
    7::7, subnet is 7::/32
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:7
    FF02::1:FF49:9
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  Input features: RPF
  Unicast RPF access-list MINI
    Process Switching:
      0 verification drops
      0 suppressed verification drops
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
```

The following is sample output for the **show ipv6 interface** command with IPv6 CEF running:

```
Router# show ipv6 interface ethernet 0/1/1

Ethernet0/1/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::203:FDFF:FE49:9
  Description: sat-2900a f0/12
  Global unicast address(es):
    7::7, subnet is 7::/32
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:7
    FF02::1:FF49:9
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  Input features: RPF
  Unicast RPF access-list MINI
```

```
  Process Switching:
    0 verification drops
    0 suppressed verification drops
  CEF Switching:
    0 verification drops
    0 suppressed verification drops
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
Hosts use stateless autoconfig for addresses.
```

Table 273 describes the significant fields shown in the display.

Table 273 show ipv6 traffic Field Descriptions

Field	Description
source-routed	Number of source-routed packets.
truncated	Number of truncated packets.
format errors	Errors that can result from checks performed on header fields, the version number, and packet length.
not a router	Message sent when IPv6 unicast routing is not enabled.
0 unicast RPF drop, 0 suppressed RPF drop	Number of unicast and suppressed reverse path forwarding (RPF) drops.
failed	Number of failed fragment transmissions.
encapsulation failed	Failure that can result from an unresolved address or try-and-queue packet.
no route	Counted when the software discards a datagram it did not know how to route.
unreach	Unreachable messages received are as follows: • routing—Indicates no route to the destination. • admin—Indicates that communication with the destination is administratively prohibited. • neighbor—Indicates that the destination is beyond the scope of the source address. For example, the source may be a local site or the destination may not have a route back to the source. • address—Indicates that the address is unreachable. • port—Indicates that the port is unreachable.
Unicast RPF access-list MINI	Unicast RPF access-list in use.
Process Switching	Displays process RPF counts, such as verification and suppressed verification drops.
CEF Switching	Displays CEF switching counts, such as verification drops and suppressed verification drops.

show ipv6 tunnel

To display IPv6 tunnel information, use the **show ipv6 tunnel** command in user EXEC or privileged EXEC mode.

show ipv6 tunnel

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(2)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 Release 12.2(14)S.
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.
12.2(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

For each tunnel running IPv6, use the **show ipv6 tunnel** command to display the tunnel unit number, the name of the dynamic routing protocol used by the tunnel, the time of last input, the number of packets in the last input, and the description string as set by the **description** command.

Examples

The following is sample output from the **show ipv6 tunnel** command:

```
Router# show ipv6 tunnel

Tun Route  LastInp  Packets
  0 RIPng    never        0
  1   -   00:00:13    55495
  2   -      never        0
  3   -   00:00:21    14755
  4   -      never        0
  5   -   00:00:00    15840
  6   -      never        0
  7   -   00:00:18    16008
  8   -      never        0
  9   -      never        0
 10   -      never        0
 11   -   00:00:03    94801
 12   -      1d02h        2
 13   -      never        0
 14   -   00:00:08   312190
```

```
15    -       never         0
16    -       never         0
17    -       never         0
18    -    00:00:05   1034954
19    -       never         0
20    -    00:00:01   1171114
21    -       never         0
```

Table 274 describes the significant fields shown in the display.

Table 274 show ipv6 tunnel Field Descriptions

Field	Description
Tun	Tunnel number.
Route	Indicates whether IPv6 RIP is enabled (RIPng) on this tunnel interface or is not enabled (-).
Last Inp	Time of last input into the tunnel.
Packets	Number of packets in this tunnel.
Description (not shown in sample output)	Description of the tunnel as entered in interface configuration mode.

show ipv6 virtual-reassembly

To display Virtual Fragment Reassembly (VFR) configuration and statistical information on a specific interface, use the **show ipv6 virtual-reassembly** command in privileged EXEC mode.

show ipv6 virtual-reassembly interface *interface-type*

Syntax Description

interface *interface-type*	Specifies the interface for which information is requested.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(7)T	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.

Usage Guidelines

This command shows the configuration and statistical information of VFR on the given interface.

Examples

The following example shows a typical display produced by this command:

```
Router# show ipv6 virtual-reassembly

All enabled IPv6 interfaces...
GigabitEthernet0/0/0:
   IPv6 Virtual Fragment Reassembly (IPV6VFR) is ENABLED [in]
   IPv6 configured concurrent reassemblies (max-reassemblies): 64
   IPv6 configured fragments per reassembly (max-fragments): 16
   IPv6 configured reassembly timeout (timeout): 3 seconds
   IPv6 configured drop fragments: OFF

   IPv6 current reassembly count:0
   IPv6 current fragment count:0
   IPv6 total reassembly count:20
   IPv6 total reassembly timeout count:0
```

The display is self-explanatory; it corresponds to the values used when you entered the **ipv6 virtual-reassembly** command.

Related Commands

Command	Description
ipv6 virtual-reassembly	Enables VFR on an interface.

show ipv6 virtual-reassembly features

To display Virtual Fragment Reassembly (VFR) information on all interfaces or on a specified interface, use the **show ipv6 virtual-reassembly features** command in privileged EXEC mode.

show ipv6 virtual-reassembly features [**interface** *interface-type*]

Syntax Description

interface *interface-type*	(Optional) Specifies the interface for which information is requested.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(7)T	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.

Usage Guidelines

This command shows the configuration and statistical information of VFR on a specified interface or on all interfaces. Use the optional **interface** *interface-type* keyword and argument to specify an interface. If you enter the **show ipv6 virtual-reassembly features** command without the keyword and argument, information about all interfaces is displayed.

Examples

The following example displays information about all interfaces:

```
Router# show ipv6 virtual-reassembly features

GigabitEthernet0/0/0:
  IPV6 Virtual Fragment Reassembly (IPV6 VFR) Current Status is ENABLED [in]
  Features to use if IPV6 VFR is Enabled:CLI
GigabitEthernet0/0/0:
  IPV6 Virtual Fragment Reassembly (IPV6 VFR) Current Status is ENABLED [out]
  Features to use if IPV6 VFR is Enabled:CLI
```

The display is self-explanatory; it corresponds to the values used when you entered the **ipv6 virtual-reassembly** command.

Related Commands

Command	Description
ipv6 virtual-reassembly	Enables VFR on an interface.
show ipv6 virtual-reassembly	Displays VFR configuration and statistical information.

show isis database

To display the Intermediate System-to-Intermediate System (IS-IS) link-state database, use the **show isis database** command in user EXEC or privileged EXEC mode.

show isis [*process-tag*] **database** [**level-1 | l1**] [**level-2 | l2**][**detail**] [**lspid**]

Syntax Description

process-tag	(Optional) A unique name among all International Organization for Standardization (ISO) router processes including IP and Connectionless Network Service (CLNS) router processes for a given router. If a process tag is specified, output is limited to the specified routing process. When **null** is specified for the process tag, output is displayed only for the router process that has no tag specified. If a process tag is not specified, output is displayed for all processes.
level-1	(Optional) Displays the IS-IS link-state database for Level 1. l1 is the abbreviation for the **level-1** keyword
level-2	(Optional) Displays the IS-IS link-state database for Level 2. l2 is the abbreviation for the **level-2** keyword.
detail	(Optional) Displays the contents of each link-state packet (LSP). Otherwise, a summary display is provided.
lspid	(Optional) Displays the link-state protocol data unit (PDU) identifier. Displays the contents of a single LSP by its ID number.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.2(15)T	Support was added for IPv6.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.0(29)S	The *process-tag* argument was 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.
12.2(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 2.4	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The order of the optional argument and keywords is not important when this command is entered. For example, the following are both valid command specifications and provide the same output: **show isis database detail l2** and **show isis database l2 detail**.

Examples

The following is sample output from the **show isis database** command:

```
Router# show isis database

IS-IS Level-1 Link State Database
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
0000.0C00.0C35.00-00  0x0000000C   0x5696        792           0/0/0
0000.0C00.40AF.00-00* 0x00000009   0x8452        1077          1/0/0
0000.0C00.62E6.00-00  0x0000000A   0x38E7        383           0/0/0
0000.0C00.62E6.03-00  0x00000006   0x82BC        384           0/0/0
0800.2B16.24EA.00-00  0x00001D9F   0x8864        1188          1/0/0
0800.2B16.24EA.01-00  0x00001E36   0x0935        1198          1/0/0

IS-IS Level-2 Link State Database
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
0000.0C00.0C35.03-00  0x00000005   0x04C8        792           0/0/0
0000.0C00.3E51.00-00  0x00000007   0xAF96        758           0/0/0
0000.0C00.40AF.00-00* 0x0000000A   0x3AA9        1077          0/0/0
```

The following is sample output from the **show isis database** command using the *process-tag* argument to display information about a VPN routing and forwarding instance (VRF)-aware IS-IS instance tagFirst:

```
Router# show isis tagFirst database level-2

Tag tagFirst:
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
igp-01.00-00          0x0000000A   0x5E73        914           0/0/0
igp-01.03-00          0x00000001   0x8E41        894           0/0/0
igp-01.04-00          0x00000001   0x8747        894           0/0/0
igp-03.00-00        * 0x00000005   0x55AD        727           0/0/0
igp-03.02-00        * 0x00000001   0x3B97        727           0/0/0
igp-02.00-0           0x00000004   0xC1FB        993           0/0/0
igp-02.01-00          0x00000001   0x448D        814           0/0/0
igp-04.00-00          0x00000004   0x76D0        892           0/0/0
```

Table 275 describes the significant fields shown in the display.

Table 275 show isis database Field Descriptions

Field	Description
Tag tagFirst	Tag name that identifies an IS-IS instance.
LSPID	The LSP identifier. The first six octets form the system ID of the router that originated the LSP. The next octet is the pseudonode ID. When this byte is nonzero, the LSP describes links from the system. When it is zero, the LSP is a so-called nonpseudonode LSP. This mechanism is similar to a router link-state advertisement (LSA) in the Open Shortest Path First (OSPF) protocol. The LSP will describe the state of the originating router. For each LAN, the designated router for that LAN will create and flood a pseudonode LSP, describing all systems attached to that LAN. The last octet is the LSP number. If there is more data than can fit in a single LSP, the LSP will be divided into multiple LSP fragments. Each fragment will have a different LSP number. An asterisk (*) indicates that the LSP was originated by the system on which this command is issued.

Table 275 show isis database Field Descriptions (continued)

Field	Description
LSP Seq Num	Sequence number for the LSP that allows other systems to determine if they have received the latest information from the source.
LSP Checksum	Checksum of the entire LSP packet.
LSP Holdtime	Amount of time the LSP remains valid (in seconds). An LSP hold time of zero indicates that this LSP was purged and is being removed from the link-state database (LSDB) of all routers. The value indicates how long the purged LSP will stay in the LSDB before being completely removed.
ATT	The Attach bit. This bit indicates that the router is also a Level 2 router, and it can reach other areas. Level 1-only routers and Level 1-2 routers that have lost connection to other Level 2 routers will use the Attach bit to find the closest Level 2 router. They will point a default route to the closest Level 2 router.
P	The P bit. Detects if the intermediate systems is area partition repair-capable. Cisco and other vendors do not support area partition repair.
OL	The Overload bit. Determines if the IS is congested. If the Overload bit is set, other routers will not use this system as a transit router when calculating routers. Only packets for destinations directly connected to the overloaded router will be sent to this router.

The following is sample output from the **show isis database detail** command:

```
Router# show isis database detail

IS-IS Level-1 Link State Database
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
0000.0C00.0C35.00-00  0x0000000C   0x5696        325           0/0/0
  Area Address: 47.0004.004D.0001
  Area Address: 39.0001
  Metric: 10   IS 0000.0C00.62E6.03
  Metric: 0    ES 0000.0C00.0C35
0000.0C00.40AF.00-00* 0x00000009   0x8452        608           1/0/0
  Area Address: 47.0004.004D.0001
  Topology: IPv4 (0x0) IPv6 (0x2)
  NLPID: 0xCC 0x8E
  IP Address: 172.16.21.49
  Metric: 10   IS 0800.2B16.24EA.01
  Metric: 10   IS 0000.0C00.62E6.03
  Metric: 0    ES 0000.0C00.40AF
  IPv6 Address: 2001:0DB8::/32
  Metric: 10   IPv6 (MT-IPv6) 2001:0DB8::/64
  Metric: 5    IS-Extended cisco.03
  Metric: 10   IS-Extended cisco1.03
  Metric: 10    IS (MT-IPv6) cisco.03
```

As the output shows, in addition to the information displayed with the **show isis database** command, the **show isis database detail** command displays the contents of each LSP.

Table 276 describes the significant fields shown in the display.

Table 276 show isis database detail Field Descriptions

Field	Description
Area Address	Reachable area addresses from the router. For Level 1 LSPs, these are the area addresses configured manually on the originating router. For Level 2 LSPs, these are all the area addresses for the area to which this router belongs.
Metric	IS-IS metric for the cost of the adjacency between the originating router and the advertised neighbor, or the metric of the cost to get from the advertising router to the advertised destination (which can be an IP address, an end system [ES], or a CLNS prefix).
Topology	States the topology supported (for example, IPv4, IPv6).
IPv6 Address	The IPv6 address.
MT-IPv6	Advertised using multitopology Type, Length, and Value objects (TLVs).

The following is additional sample output from the **show isis database detail** command. This LSP is a Level 2 LSP. The area address 39.0001 is the address of the area in which the router resides.

```
Router# show isis database l2 detail

IS-IS Level-2 Link State Database
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
0000.0C00.1111.00-00* 0x00000006   0x4DB3        1194          0/0/0
  Area Address: 39.0001
  NLPID:        0x81 0xCC
  IP Address:  172.16.64.17
  Metric: 10   IS 0000.0C00.1111.09
  Metric: 10   IS 0000.0C00.1111.08
  Metric: 10   IP 172.16.65.0 255.255.255.0
```

show isis ipv6 rib

To display the IPv6 local Routing Information Base (RIB), use the **show isis ipv6 rib** command in user EXEC or privileged EXEC mode.

show isis ipv6 rib [*ipv6-prefix*]

no show isis ipv6 rib [*ipv6-prefix*]

Syntax Description

ipv6-prefix	(Optional) IPv6 address prefix. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

Command Modes

User EXEC
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(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.
12.2(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 2.6	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

When the optional *ipv6-prefix* argument is not used, the complete Intermediate System-to-Intermediate System (IS-IS) IPv6 RIB is displayed. When an optional IPv6 prefix is supplied, only the entry matching that prefix is displayed.

Only the optimal paths will be installed in the master IPv6 RIB as IS-IS routes.

Examples

The following is sample output from the **show isis ipv6 rib** command. An asterisk (*) indicates prefixes that have been installed in the master IPv6 RIB as IS-IS routes. Following each prefix is a list of all paths in order of preference, with optimal paths listed first and suboptimal paths listed after optimal paths.

```
Router# show isis ipv6 rib

IS-IS IPv6 process "", local RIB
  88:1::/64
    via FE80::210:7BFF:FEC2:ACC9/Ethernet2/0, type L2  metric 20 LSP [3/7]
    via FE80::210:7BFF:FEC2:ACCC/Ethernet2/1, type L2  metric 20 LSP [3/7]
* 1357:1::/64
    via FE80::202:7DFF:FE1A:9471/Ethernet2/1, type L2  metric 10 LSP [4/9]
* 2001:45A::/64
```

```
via FE80::210:7BFF:FEC2:ACC9/Ethernet2/0, type L1  metric 20 LSP [C/6]
via FE80::210:7BFF:FEC2:ACCC/Ethernet2/1, type L1  metric 20 LSP [C/6]
via FE80::210:7BFF:FEC2:ACC9/Ethernet2/0, type L2  metric 20 LSP [3/7]
via FE80::210:7BFF:FEC2:ACCC/Ethernet2/1, type L2  metric 20 LSP [3/7]
```

Table 277 describes the significant fields shown in the display.

Table 277 show isis ipv6 rib Field Descriptions

Field	Description
*	Prefixes that have been installed in the master IPv6 RIB as IS-IS routes.
type	Type of path: • L1—Level 1 • L2—Level 2 • IA—Inter-area • Sum—Summary
LSP [3/7]	Link-state packet (LSP). The numbers following LSP indicate the LSP index and LSP version, respectively.

show isis spf-log

To display how often and why the router has run a full shortest path first (SPF) calculation, use the **show isis spf-log** command in privileged EXEC mode.

show isis [*area-tag*] [**ipv6** | *] **spf-log** [**topology** {**ipv6** | *topology-name* | *}]

Syntax Description

area-tag	(Optional) Required for multiarea Intermediate System-to-Intermediate System (IS-IS) configuration. Optional for conventional IS-IS configuration. Meaningful name for a routing process. This name must be unique among all IP or Connectionless Network Service (CLNS) router processes for a given router. If an area tag is not specified, a null tag is assumed and the process is referenced with a null tag. If an area tag is specified, output is limited to the specified area.
ipv6	(Optional) Displays the IS-IS multitopology for IPv6 SPF log.
*	(Optional) Displays the SPF logs of all address families.
topology	(Optional) Specifies the Multiple Transport Stream Receiver (MTR) topology.
topology-name	(Optional) The IS-IS multitopology SPF log for the specified topology name.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.2(15)T	Support was added for IPv6.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)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 2.4	This command was introduced on Cisco ASR 1000 Series Aggregation Services Routers.

Examples

The following is sample output from the **show isis spf-log** command with the optional **ipv6** keyword:

```
Router# show isis ipv6 spf-log

                IPv6 Level 1 SPF log
  When   Duration  Nodes  Count     Last trigger LSP   Triggers
00:15:46    3124     40      1          milles.00-00  TLVCODE
00:15:24    3216     41      5          milles.00-00  TLVCODE NEWLSP
00:15:19    3096     41      1          deurze.00-00  TLVCODE
```

```
00:14:54    3004     41      2          milles.00-00  ATTACHFLAG LSPHEADER
00:14:49    3384     41      1          milles.00-01  TLVCODE
00:14:23    2932     41      3          milles.00-00  TLVCODE
00:05:18    3140     41      1                        PERIODIC
00:03:54    3144     41      1          milles.01-00  TLVCODE
00:03:49    2908     41      1          milles.01-00  TLVCODE
00:03:28    3148     41      3           bakel.00-00  TLVCODE TLVCONTENT
00:03:15    3054     41      1          milles.00-00  TLVCODE
00:02:53    2958     41      1          mortel.00-00  TLVCODE
00:02:48    3632     41      2          milles.00-00  NEWADJ TLVCODE
00:02:23    2988     41      1          milles.00-01  TLVCODE
00:02:18    3016     41      1          gemert.00-00  TLVCODE
00:02:14    2932     41      1           bakel.00-00  TLVCONTENT
00:02:09    2988     41      2           bakel.00-00  TLVCONTENT
00:01:54    3228     41      1          milles.00-00  TLVCODE
00:01:38    3120     41      3            rips.03-00  TLVCONTENT
```

Table 278 describes the significant fields shown in the display.

Table 278 show isis spf-log Field Descriptions

Field	Description
When	How long ago (in hours: minutes: seconds) a full SPF calculation occurred. The last 20 occurrences are logged.
Duration	Number of milliseconds required to complete this SPF run. Elapsed time is wall clock time, not CPU time.
Nodes	Number of routers and pseudonodes (LANs) that make up the topology calculated in this SPF run.
Count	Number of events that triggered this SPF run. When there is a topology change, often multiple link-state packets (LSPs) are received in a short time. A router waits 5 seconds before running a full SPF run, so it can include all new information. This count denotes the number of events (such as receiving new LSPs) that occurred while the router was waiting its 5 seconds before running full SPF.
Last trigger LSP	Whenever a full SPF calculation is triggered by the arrival of a new LSP, the router stores the LSP ID. The LSP ID can provide a clue as to the source of routing instability in an area. If multiple LSPs are causing an SPF run, only the LSP ID of the last received LSP is remembered.
Triggers	A list of all reasons that triggered a full SPF calculation. For a list of possible triggers, see Table 279.

Table 279 lists possible triggers of a full SPF calculation.

Table 279 Possible Triggers of Full SPF Calculation

Trigger	Description
ADMINDIST	Another administrative distance was configured for the IS-IS process on this router.
AREASET	Set of learned area addresses in this area changed.
ATTACHFLAG	This router is now attached to the Level 2 backbone or it has just lost contact to the Level 2 backbone.

Table 279 Possible Triggers of Full SPF Calculation (continued)

Trigger	Description
BACKUPOVFL	An IP prefix disappeared. The router knows there is another way to reach that prefix but has not stored that backup route. The only way to find the alternative route is through a full SPF run.
DBCHANGED	A **clear isis *** command was issued on this router.
IPBACKUP	An IP route disappeared, which was not learned via IS-IS, but via another protocol with better administrative distance. IS-IS will run a full SPF to install an IS-IS route for the disappeared IP prefix.
IPQUERY	A **clear ip route** command was issued on this router.
LSPEXPIRED	Some LSP in the link-state database (LSDB) has expired.
LSPHEADER	ATT/P/OL bits or is-type in an LSP header changed.
NEWADJ	This router has created a new adjacency to another router.
NEWAREA	A new area (via network entity title [NET]) was configured on this router.
NEWLEVEL	A new level (via is-type) was configured on this router.
NEWLSP	A new router or pseudonode appeared in the topology.
NEWMETRIC	A new metric was configured on an interface of this router.
NEWSYSID	A new system ID (via NET) was configured on this router.
PERIODIC	Typically, every 15 minutes a router runs a periodic full SPF calculation.
RTCLEARED	A **clear clns route** command was issued on this router.
TLVCODE	TLV code mismatch, indicating that different type length values (TLVs) are included in the newest version of an LSP.
TLVCONTENT	TLV contents changed. This normally indicates that an adjacency somewhere in the area has come up or gone down. The “Last trigger LSP” column indicates where the instability may have occurred.

show isis topology

To display a list of all connected routers in all areas, use the **show isis topology** command in user EXEC or privileged EXEC mode.

show isis [*process-tag*] [**ipv6** | *] **topology** [*hostname*] [**level-1** | **level-2** | **l1** | **l2**]

Syntax Description

process-tag	(Optional) A unique name among all International Organization for Standardization (ISO) router processes including IP and Connectionless Network Service (CLNS) router processes for a given router. If a process tag is specified, output is limited to the specified routing process. When **null** is specified for the process tag, output is displayed only for the router process that has no tag specified. If a process tag is not specified, output is displayed for all processes.
ipv6	(Optional) Displays Intermediate System-to-Intermediate System (IS-IS) IPv6 topology.
*	(Optional) Displays the topology of all address families.
hostname	(Optional) Hostname or the Network Service Access Point (NSAP) address of the router.
level-1	(Optional) Specifies paths to all level one routers in the area.
level-2	(Optional) Specifies paths to all level two routers in the domain.
l1	(Optional) Abbreviation for the **level-1** keyword.
l2	(Optional) Abbreviation for the **level-2** keyword.

Command Modes

Privileged EXEC (#)

Command History

OS Release	Modification
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.0(29)S	This command was modified. The *process-tag* argument was added.
S Release	**Modification**
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
SB Release	**Modification**
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
SG Release	**Modification**
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
SX Release	**Modification**
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Mainline and T Release	**Modification**
12.0(5)T	This command was introduced.
12.2(15)T	This command was modified. Support was added for IPv6.
XE Release	**Modification**
Cisco IOS XE Release 2.4	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

Use the **show isis topology** command to verify the presence and connectivity between all routers in all IS-IS areas.

If you are running Cisco IOS Release 12.2(33)SRB or a later release, use the **show isis topology** (MTR) command.

Examples

The following is sample output from the **show isis topology** command using the optional **ipv6** keyword. The command shown is used in a dual CLNS-IP network:

```
Router# show isis ipv6 topology

Tag L2BB:
IS-IS IPv6 paths to level-1 routers
System Id       Metric  Next-Hop        Interface       SNPA
0000.0000.0005 --
0000.0000.0009  10      0000.0000.0009  Tu529           *Tunnel*
0000.0000.0017  20      0000.0000.0009  Tu529           *Tunnel*
0000.0000.0053  30      0000.0000.0009  Tu529           *Tunnel*
0000.0000.0068  20      0000.0000.0009  Tu529           *Tunnel*

IS-IS paths to level-2 routers
System Id       Metric  Next-Hop        Interface       SNPA
0000.0000.0005  --
0000.0000.0009  10      0000.0000.0009  Tu529           *Tunnel*
0000.0000.0017  20      0000.0000.0009  Tu529           *Tunnel*
0000.0000.0053  30      0000.0000.0009  Tu529           *Tunnel*
0000.0000.0068  20      0000.0000.0009  Tu529           *Tunnel*
Tag A3253-01:
IS-IS paths to level-1 routers
System Id       Metric  Next-Hop        Interface       SNPA
0000.0000.0003  10      0000.0000.0003  Et1             0000.0c03.6944
0000.0000.0005  --
```

```
0000.0000.0053  10      0000.0000.0053  Et1             0060.3e58.ccdb

Tag A3253-02:
IS-IS paths to level-1 routers
System Id       Metric  Next-Hop        Interface       SNPA
0000.0000.0002  10      0000.0000.0002  Et2             0000.0c03.6bc5
0000.0000.0005  --
0000.0000.0053  10      0000.0000.0053  Et2             0060.3e58.ccde
```

Table 280 describes the significant fields shown in the display.

Table 280 show isis topology Field Descriptions

Field	Description
Tag	Identifies the routing process.
System Id	Six-byte value that identifies a system in an area.
Metric	IS-IS metric for the cost of the adjacency between the originating router and the advertised neighbor, or the metric of the cost to get from the advertising router to the advertised destination (which can be an IP address, an end system [ES], or a CLNS prefix).
Next-Hop	The address of the next hop router.
Interface	Interface from which the system was learned.
SNPA	Subnetwork point of attachment. This is the data-link address.

Related Commands

Command	Description
show clns es-neighbors	Lists the ES neighbors that this router knows.
show clns is-neighbors	Displays IS-IS related information for IS-IS router adjacencies.
show clns neighbors	Displays the ES, IS, and M-ISIS neighbors.
show clns neighbor areas	Displays information about IS-IS neighbors and the areas to which they belong.
show clns route	Displays one or all of the destinations to which the router knows how to route CLNS packets.

show key chain

To display authentication key information, use the **show key chain** command in EXEC mode.

show key chain [*name-of-chain*]

Syntax Description

name-of-chain	(Optional) Name of the key chain to display, as named in the **key chain** command.

Defaults

Information about all key chains is displayed.

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.

Examples

The following is sample output from the **show key chain** command:

```
Router# show key chain

Key-chain trees:
    key 1 -- text "chestnut"
        accept lifetime (always valid) - (always valid) [valid now]
        send lifetime (always valid) - (always valid) [valid now]
    key 2 -- text "birch"
        accept lifetime (00:00:00 Dec 5 1995) - (23:59:59 Dec 5 1995)
        send lifetime (06:00:00 Dec 5 1995) - (18:00:00 Dec 5 1995)
```

Related Commands

Command	Description
accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.
key	Identifies an authentication key on a key chain.
key chain	Enables authentication for routing protocols.
key-string (authentication)	Specifies the authentication string for a key.
send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.

show l2tp session

To display information about Layer 2 Tunneling Protocol (L2TP) sessions, use the **show l2tp session** command in privileged EXEC mode.

show l2tp session [**all** | **packets** [**ipv6**] | **sequence** | **state** | [**brief** | **circuit** | **interworking**] [**hostname**]] [**ip-addr** *ip-addr* [**vcid** *vcid*] | **tunnel** {**id** *local-tunnel-id local-session-id* | **remote-name** *remote-tunnel-name local-tunnel-name*} | **username** *username* | **vcid** *vcid*]

Syntax Description

all	(Optional) Displays information for all active sessions.
packets	(Optional) Displays information about packet or byte counts for sessions.
ipv6	(Optional) (Optional) Displays IPv6 packet and byte-count statistics.
sequence	(Optional) Displays sequence information for sessions.
state	(Optional) Displays state information for sessions.
brief	(Optional) Displays brief session information.
circuit	(Optional) Displays the Layer 2 circuit information.
interworking	(Optional) Displays interworking information.
hostname	(Optional) Displays output using L2TP control channel hostnames rather than IP addresses
ip-addr *ip-addr*	(Optional) Specifies the peer IP address associated with the session.
vcid *vcid*	(Optional) Specifies the Virtual Circuit ID (VCID) associated with the session. The range is from 1 to 4294967295.
tunnel	(Optional) Displays the sessions in a tunnel.
id *local-tunnel-id local-session-id*	Specifies the session by tunnel ID and session ID. The range for the local tunnel ID and local session ID is from 1 to 4294967295.
remote-name *remote-tunnel-name local-tunnel-name*	Specifies the remote names for the remote and local L2TP tunnels.
username *username*	(Optional) Specifies the username associated with the session.

Command Modes

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.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
Cisco IOS XE Release 2.6	The **ipv6** keyword was added. The **show l2tp session** command with the **all** keyword was modified to display IPv6 counter information.

Usage Guidelines

To use the **show l2tp session** command, you must configure the following commands:

- The **vpdn enable** command in global configuration mode
- The **vpdn-group** command in global configuration mode
- The **request-dialin** command in VPDN group configuration mode
- The **protocol** command in request dial-in VPDN subgroup configuration mode
- The **domain** command in request dial-in VPDN subgroup configuration mode
- The **initiate-to** command in VPDN group configuration mode
- The **local name** command in VPDN group configuration mode
- The **l2tp tunnel password** command in VPDN group configuration mode
- The **l2tp attribute clid mask-method** command in VPDN group configuration mode

Examples

The following is sample output from the **show l2tp session** command:

```
Router# show l2tp session packets

L2TP Session Information Total tunnels 1 sessions 2

LocID      RemID      TunID      Pkts-In    Pkts-Out   Bytes-In   Bytes-Out
18390      313101640  4059745793 0          0          0          0
25216      4222832574 4059745793 15746      100000     1889520    12000000
```

Related Commands

Command	Description
domain (isakmp-group)	Specifies the DNS domain to which a group belongs and enters the ISAKMP group configuration mode.
initiate-to	Specifies an IP address used for Layer 2 tunneling.
local name	Specifies a local hostname that the tunnel uses to identify itself.
l2tp attribute clid mask-method	Configures a NAS to suppress L2TP calling station IDs for sessions associated with a VPDN group or VPDN template and enters a VPDN group or VPDN template configuration mode.
l2tp tunnel password	Sets the password the router uses to authenticate L2TP tunnels.
protocol (L2TP)	Specifies the signaling protocol to be used to manage the pseudowires created from a pseudowire class for a Layer 2 session and to cause control plane configuration settings to be taken from a specified L2TP class.
request-dialin	Creates a request dial-in VPDN subgroup that configures a NAS to request the establishment of a dial-in tunnel to a tunnel server, and enters request dial-in VPDN subgroup configuration mode.
vpdn enable	Enables VPDN on the router and informs the router to look for tunnel definitions in a local database and on a remote authorization server (home gateway), if one is present.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.

show l2tp tunnel

To display details about Layer 2 Tunneling Protocol (L2TP) tunnels, use the **show l2tp tunnel** command in privileged EXEC mode.

show l2tp tunnel [**all** | **packets** [**ipv6**] | **state** | **summary** | **transport**] [**id** *local-tunnel-id* | **local-name** *local-tunnel-name remote-tunnel-name* | **remote-name** *remote-tunnel-name local-tunnel-name*]

Syntax Description

all	(Optional) Displays information about all active tunnels.
packets	(Optional) Displays information about packet or byte counts.
ipv6	(Optional) Displays IPv6 packet and byte-count statistics.
state	(Optional) Displays the state of the tunnel.
summary	(Optional) Displays a summary of the tunnel information.
transport	(Optional) Displays tunnel transport information.
id *local-tunnel-id*	(Optional) Specifies the local tunnel ID of the L2TP tunnel. The range is from 1 to 4294967295.
local-name *local-tunnel-name remote-tunnel-name*	(Optional) Specifies the local names for the local and remote L2TP tunnels.
remote-name *remote-tunnel-name local-tunnel-name*	(Optional) Specifies the remote names for the remote and local L2TP tunnels.

Command Modes

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.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
Cisco IOS XE Release 2.6	The **ipv6** keyword was added. The **show l2tp tunnel** command with the **all** keyword was modified to display IPv6 counter information.

Usage Guidelines

To use the **show l2tp tunnel** command, you must configure the following commands:

- The **vpdn enable** command in global configuration mode
- The **vpdn-group** command in global configuration mode
- The **request-dialin** command in VPDN group configuration mode
- The **protocol** command in request dial-in VPDN subgroup configuration mode
- The **domain** command in request dial-in VPDN subgroup configuration mode

- The **initiate-to** command in VPDN group configuration mode
- The **local name** command in VPDN group configuration mode
- The **l2tp tunnel password** command in VPDN group configuration mode
- The **l2tp attribute clid mask-method** command in VPDN group configuration mode

Depending on the keywords or arguments entered, the **show l2tp tunnel** command displays information such as packet or byte count, state, transport, local or remote names, and summary information for L2TP tunnels.

Examples

The following is sample output from the **show l2tp tunnel** command:

```
Router# show l2tp tunnel all

L2TP Tunnel Information Total tunnels 1 sessions 1 Tunnel id 746420372 is up, remote id is
2843347489, 1 active sessions
 Remotely initiated tunnel
 Tunnel state is established, time since change 00:30:16  Tunnel transport is IP (115)
 Remote tunnel name is 7604-AA1705
  Internet Address 12.27.17.86, port 0
 Local tunnel name is 7606-AA1801
  Internet Address 12.27.18.86, port 0
 L2TP class for tunnel is l2tp_default_class
 Counters, taking last clear into account:
  598 packets sent, 39 received
  74053 bytes sent, 15756 received
  Last clearing of counters never
 Counters, ignoring last clear:
  598 packets sent, 39 received
  74053 bytes sent, 15756 received
 Control Ns 3, Nr 35
 Local RWS 1024 (default), Remote RWS 1024
 Control channel Congestion Control is disabled
 Tunnel PMTU checking disabled
 Retransmission time 1, max 1 seconds
 Unsent queuesize 0, max 0
 Resend queuesize 0, max 1
 Total resends 0, ZLB ACKs sent 33
 Total out-of-order dropped pkts 0
 Total out-of-order reorder pkts 0
 Total peer authentication failures 0
 Current no session pak queue check 0 of 5
 Retransmit time distribution: 0 0 0 0 0 0 0 0 0
 Control message authentication is disabled
```

Related Commands

Command	Description
domain (isakmp-group)	Specifies the DNS domain to which a group belongs and enters the ISAKMP group configuration mode.
initiate-to	Specifies an IP address used for Layer 2 tunneling.
local name	Specifies a local hostname that the tunnel uses to identify itself.
l2tp attribute clid mask-method	Configures a NAS to suppress L2TP calling station IDs for sessions associated with a VPDN group or VPDN template and enters a VPDN group or VPDN template configuration mode.
l2tp tunnel password	Sets the password the router uses to authenticate L2TP tunnels.

Command	Description
protocol (L2TP)	Specifies the signaling protocol to be used to manage the pseudowires created from a pseudowire class for a Layer 2 session and to cause control plane configuration settings to be taken from a specified L2TP class.
request-dialin	Creates a request dial-in VPDN subgroup that configures a NAS to request the establishment of a dial-in tunnel to a tunnel server, and enters request dial-in VPDN subgroup configuration mode.
vpdn enable	Enables VPDN on the router and informs the router to look for tunnel definitions in a local database and on a remote authorization server (home gateway), if one is present.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.

show l2tun session

To display the current state of Layer 2 sessions and protocol information about Layer 2 Tunnel Protocol (L2TP) control channels, use the **show l2tun session** command in privileged EXEC mode.

show l2tun session [**l2tp** | **pptp**] [**all** [*filter*] | **brief** [*filter*] [**hostname**] | **circuit** [*filter*] [**hostname**] | **interworking** [*filter*] [**hostname**] | **packets** [**ipv6**] [*filter*] | **sequence** [*filter*] | **state** [*filter*]]

Syntax Descriptions

l2tp	(Optional) Displays information about L2TP.
pptp	(Optional) Displays information about Point-to-Point Tunneling Protocol.
all	(Optional) Displays information about all current L2TP sessions on the router.
filter	(Optional) One of the filter parameters defined in Table 281.
brief	(Optional) Displays information about all current L2TP sessions, including the peer ID address and circuit status of the L2TP sessions.
hostname	(Optional) Specifies that the peer hostname will be displayed in the output.
circuit	(Optional) Displays information about all current L2TP sessions, including circuit status (up or down).
interworking	(Optional) Displays information about Layer 2 Virtual Private Network (L2VPN) interworking.
packets	(Optional) Displays information about the packet counters (in and out) associated with current L2TP sessions.
ipv6	(Optional) Displays IPv6 packet and byte-count statistics.
sequence	(Optional) Displays sequencing information about each L2TP session, including the number of out-of-order and returned packets.
state	(Optional) Displays information about all current L2TP sessions and their protocol state, including remote Virtual Connection Identifiers (VCIDs).

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.0(31)S	The **hostname** keyword was 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.
12.4(11)T	This command 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.
12.4(22)T	This command was modified.The **pptp** and **tunnel** keywords were added.
Cisco IOS XE Release 2.6	The **ipv6** keyword was added. The **show l2tun session** command with the **all** and **l2tp all** keywords was modified to display IPv6 counter information.

Usage Guidelines

Use the **show l2tun session** command to display information about current L2TP sessions on the router.

Table 281 defines the filter parameters available to refine the output of the **show l2tun session** command.

Table 281 Filter Parameters for the show l2tun session Command

Syntax	Description
ip-addr *ip-address* [**vcid** *number*]	Filters the output to display information about only those L2TP sessions associated with the IP address of the peer router. The 32-bit VCID shared between the peer router and the local router at each end of the control channel can be optionally specified. • *ip-address*—IP address of the peer router. • *number*—VCID number.
vcid *number*	Filters the output to display information about only those L2TP sessions associated with the VCID shared between the peer router and the local router at each end of the control channel. • *number*—VCID number.
username *username*	Filters the output to display information for only those sessions associated with the specified username. • *username*—Username.
tunnel {**id** *local-tunnel local-session* | **remote-name** *remote-tunnel local-tunnel-name*}	Displays the sessions in a tunnel. • **id**—Tunnel ID for established tunnels. • *local-tunnel*—Local tunnel ID. • *local-session*—Local session ID. • **remote-name**—Remote tunel name. • *remote-tunnel*—Remote tunnel name. • *local-tunnel*—Local tunnel name.

Examples

The following example shows how to display detailed information about all current L2TP sessions:

```
Router# show l2tun session all

Session Information Total tunnels 0 sessions 1

Session id 42438 is down, tunnel id n/a
  Remote session id is 0, remote tunnel id n/a
Session Layer 2 circuit, type is Ethernet, name is FastEthernet4/1/1
  Session vcid is 123456789
  Circuit state is DOWN
    Local circuit state is DOWN
    Remote circuit state is DOWN
Call serial number is 1463700128
Remote tunnel name is PE1
  Internet address is 10.1.1.1
Local tunnel name is PE1
  Internet address is 10.1.1.2
IP protocol 115
  Session is L2TP signalled
  Session state is idle, time since change 00:00:26
    0 Packets sent, 0 received
```

```
    0 Bytes sent, 0 received
  Last clearing of "show vpdn" counters never
    Receive packets dropped:
      out-of-order:            0
      total:                   0
    Send packets dropped:
      exceeded session MTU:    0
      total:                   0
  DF bit off, ToS reflect disabled, ToS value 0, TTL value 255
  No session cookie information available
  UDP checksums are disabled
  L2-L2 switching enabled
  No FS cached header information available
  Sequencing is off
  Unique ID is 1
```

The following example shows how to display information only about the L2TP session set up on a peer router with an IP address of 192.0.2.0 and a VCID of 300:

```
Router# show l2tun session all ip-addr 192.0.2.0 vcid 300

L2TP Session
Session id 32518 is up, tunnel id n/a
Call serial number is 2074900020
Remote tunnel name is tun1
  Internet address is 192.0.2.0
Session is L2TP signalled
  Session state is established, time since change 03:06:39
    9932 Packets sent, 9932 received
    1171954 Bytes sent, 1171918 received
  Session vcid is 300
  Session Layer 2 circuit, type is Ethernet Vlan, name is FastEthernet0/1/0.3:3
  Circuit state is UP
    Remote session id is 18819, remote tunnel id n/a
  Set DF bit to 0
  Session cookie information:
    local cookie, size 4 bytes, value CF DC 5B F3
    remote cookie, size 4 bytes, value FE 33 56 C4
  SSS switching enabled
  Sequencing is on
    Ns 9932, Nr 10001, 0 out of order packets discarded
```

Table 282 describes the significant fields shown in the displays.

Table 282 show l2tun session Field Descriptions

Field	Description
Total tunnels	Total number of L2TP tunnels established on the router.
sessions	Number of L2TP sessions established on the router.
Session id	Session ID for established sessions.
is	Session state.
tunnel id	Tunnel ID for established tunnels.
Remote session id	Session ID for the remote session.
tunnel id	Tunnel ID for the remote tunnel.
Session Layer 2 circuit, type is, name is	Type and name of the interface used for the Layer 2 circuit.

Table 282 show l2tun session Field Descriptions (continued)

Field	Description
Session vcid is	VCID of the session.
Circuit state is	State of the Layer 2 circuit.
Local circuit state is	State of the local circuit.
Remote circuit state is	State of the remote circuit.
Call serial number is	Call serial number.
Remote tunnel name is	Name of the remote tunnel.
Internet address is	IP address of the remote tunnel.
Local tunnel name is	Name of the local tunnel.
Internet address is	IP address of the local tunnel.
IP protocol	The IP protocol used.
Session is	Signaling type for the session.
Session state is	Session state for the session.
time since change	Time since the session state last changed, in the format hh:mm:ss.
Packets sent, received	Number of packets sent and received since the session was established.
Bytes sent, received	Number of bytes sent and received since the session was established.
Last clearing of "show vpdn" counters	Time elapsed since the last clearing of the counters displayed with the **show vpdn** command. Time will be displayed in one of the following formats: • hh:mm:ss—Hours, minutes, and seconds. • dd:hh—Days and hours. • WwDd—Weeks and days, where W is the number of weeks and D is the number of days. • YyWw—Years and weeks, where Y is the number of years and W is the number of weeks. • never—The timer has not been started.
Receive packets dropped:	Number of received packets that were dropped since the session was established. • out-of-order—Total number of received packets that were dropped because they were out of order. • total—Total number of received packets that were dropped.
Send packets dropped:	Number of sent packets that were dropped since the session was established. • exceeded session MTU—Total number of sent packets that were dropped because the session maximum transmission unit (MTU) was exceeded. • total—Total number of sent packets that were dropped.
DF bit	Status of the Don't Fragment (DF) bit option. The DF bit can be on or off.
ToS reflect	Status of the type of service (ToS) reflect option. ToS reflection can be enabled or disabled.
ToS value	Value of the ToS byte in the L2TP header.

Table 282 show l2tun session Field Descriptions (continued)

Field	Description
TTL value	Value of the time-to-live (TTL) byte in the L2TP header.
local cookie	Size (in bytes) and value of the local cookie.
remote cookie	Size (in bytes) and value of the remote cookie.
UDP checksums are	Status of the User Datagram Protocol (UDP) checksum configuration.
switching	Status of switching.
No FS cached header information available	Fast Switching (FS) cached header information. If an FS header is configured, the encapsulation size and hexadecimal contents of the FS header will be displayed. The FS header is valid only for IP virtual private dialup network (VPDN) traffic from a tunnel server to a network access server (NAS).
Sequencing is	Status of sequencing. Sequencing can be on or off.
Ns	Sequence number for sending.
Nr	Sequence number for receiving.
Unique ID is	Global user ID correlator.

The following example shows how to display information about the circuit status of L2TP sessions on a router:

```
Router# show l2tun session circuit

Session Information Total tunnels 3 sessions 3

LocID      TunID      Peer-address    Type Stat Username, Intf/
                                                Vcid, Circuit
32517      n/a         172.16.184.142  VLAN UP   100, Fa0/1/0.1:1
32519      n/a         172.16.184.142  VLAN UP   200, Fa0/1/0.2:2
32518      n/a         172.16.184.142  VLAN UP   300, Fa0/1/0.3:3
```

The following example shows how to display information about the circuit status of L2TP sessions and the hostnames of remote peers:

```
Router# show l2tun session circuit hostname

Session Information Total tunnels 3 sessions 3

LocID      TunID      Peer-hostname Type Stat Username, Intf/
                                                Vcid, Circuit
32517      n/a         <unknown>       VLAN UP   100, Fa0/1/0.1:1
32519      n/a         router32        VLAN UP   200, Fa0/1/0.2:2
32518      n/a         access3         VLAN UP   300, Fa0/1/0.3:3
```

Table 283 describes the significant fields shown in the displays.

Table 283 show l2tun session circuit Field Descriptions

Field	Description
LocID	Local session ID.
TunID	Tunnel ID.
Peer-address	IP address of the peer.
Peer-hostname	Hostname of the peer.

Table 283 show l2tun session circuit Field Descriptions (continued)

Field	Description
Type	Session type.
Stat	Session status.
Username, Intf/Vcid, Circuit	Username, interface name/VCID, and circuit number of the session.

Related Commands

Command	Description
show l2tun	Displays general information about Layer 2 tunnels and sessions.
show l2tun tunnel	Displays the current state of Layer 2 tunnels and information about configured tunnels.

show mls cef ipv6

To display the hardware IPv6-switching table entries, use the **show mls cef ipv6** command in privileged EXEC mode.

show mls cef ipv6 [**vrf** *vrf-name*] [*ip-address*/*mask*] [**accounting per-prefix**] [**module** *number*]

show mls cef ipv6 exact-route *src-addr* [*L4-src-port*] *dst-addr* [*L4-dst-port*]

show mls cef ipv6 multicast tcam [*v6mcast-address*] [**detail**] [**internal**]

Syntax Description

vrf	(Optional) IPv6 Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) VRF name.
ip-address/*mask*	(Optional) Entry IPv6 address and prefix mask. Valid values for the *mask* argument are from 0 through 128.
accounting per-prefix	(Optional) Displays per-prefix accounting statistics.
module *number*	(Optional) Displays the entries for a specific module.
exact-route	Provides the exact route of IPv6-switching table entries.
src-addr	Source IP address.
L4-src-port	(Optional) Layer 4-source port number; valid values are from 0 to 65535.
dst-addr	Destination IP address.
L4-dst-port	(Optional) Layer 4-destination port number; valid values are from 0 to 65535.
multicast tcam	Displays IPv6-multicast entries.
v6mcast-address	(Optional) IPv6-multicast address.
detail	(Optional) Displays detailed hardware information.
internal	(Optional) *Displays internal hardware information.*

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(17a)SX	This command was introduced on the Supervisor Engine 720.
12.2(17b)SXA	The output was changed to display multicast protocol information in the Forwarding Information Base (FIB) driver.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB1	This command was integrated into Cisco IOS Release 12.2(33)SRB1.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

You can enter this command on the supervisor engine and Multilayer Switching (MLS)-hardware Layer 3-switching module consoles only. Enter the **remote login** command to enter a session into the supervisor engine and distributed forwarding card (DFC)-equipped module to enter the commands.

When entering the *ip-address/mask* argument, use this format, X:X:X:X::X/*mask,* where valid values for *mask* are from 0 to 128.

Up to 64 IPv6 prefixes are supported.

You must enter the *L4-src-port* and *L4-dst-port* arguments when the load-sharing mode is set to full, for example, when Layer 4 ports are included in the load-sharing hashing algorithm.

Examples

This example shows how to display the hardware IPv6-switching table entries:

```
Router# show mls cef ipv6

Codes:M-MPLS encap, + - Push label
Index Prefix Adjacency
524384 BEEF:6::6/128 punt
524386 5200::6/128 punt
524388 2929::6/128 punt
524390 6363::30/128 Fa1/48 , 0000.0001.0002
524392 3FFE:1B00:1:1:0:5EFE:1B00:1/128 punt
524394 2002:2929:6:2::6/128 punt
524396 2002:2929:6:1::6/128 punt
524398 6363::6/128 punt
524416 BEEF:6::/64 drop
524418 5200::/64 punt
524420 2929::/64 punt
524422 2002:2929:6:2::/64 punt
524424 2002:2929:6:1::/64 punt
524426 6363::/64 punt
524428 3FFE:1B00:1:1::/64 Tu4 , V6 auto-tunnel
524448 FEE0::/11 punt
524480 FE80::/10 punt
524512 FF00::/8 punt
524544 ::/0 drop
```

This example shows how to display the IPv6 entries for a specific IPv6 address and mask:

```
Router# show mls cef ipv6 2001:4747::/64

Codes:R - Recirculation, I-IP encap
M-MPLS encap, + - Push label
Index Prefix Out i/f Out Label
160 2001:4747::/64 punt
```

This example shows how to display all the IPv6-FIB entries that have per-prefix statistics available:

```
Router# show mls cef ipv6 accounting per-prefix

(I) BEEF:2::/64: 0 packets, 0 bytes

A - Active, I - Inactive
```

This example shows how to display detailed hardware information:

```
Router# show mls cef ipv6 detail

Codes: M - mask entry, V - value entry, A - adjacency index, P - FIB Priority
D - FIB Don't short-cut, m - mod-num
Format: IPv6_DA - (C | xtag vpn uvo prefix)
M(128 ): F | 1 FF 1 FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
```

```
V(128 ): C | 1 0 1 2001:4747::1253 (A:12 ,P:1,D:0,m:0 )
M(160 ): F | 1 FF 1 FFFF:FFFF:FFFF:FFFF::
V(160 ): C | 1 0 1 2001:4747:: (A:11 ,P:1,D:0,m:0 )
M(224 ): F | 1 FF 1 FFE0::
V(224 ): C | 1 0 1 FEE0:: (A:11 ,P:1,D:0,m:0 )
M(256 ): F | 1 FF 1 FFC0::
V(256 ): C | 1 0 1 FE80:: (A:12 ,P:1,D:0,m:0 )
M(352 ): F | 1 FF 1 FF00::
V(352 ): C | 1 0 1 FF00:: (A:12 ,P:1,D:0,m:0 )
M(480 ): F | 1 FF 1 ::
V(480 ): C | 1 0 1 :: (A:14 ,P:1,D:0,m:0
```

Related Commands

Command	Description
mls ipv6 acl compress address unicast	Turns on the compression of IPv6 addresses.
remote login	Accesses the Cisco 7600 series router console or a specific module.

show mls netflow ipv6

To display information about the hardware NetFlow IPv6 configuration, use the **show mls netflow ipv6** command in privileged EXEC mode.

show mls netflow ipv6 any

show mls netflow ipv6 count [**module** *number*]

show mls netflow ipv6 destination *ipv6-address*[*/ipv6-prefix*] [**count** [**module** *number*] | **detail** | **dynamic** | **flow** {**icmp** | **tcp** | **udp**} | **module** *number* | **nowrap** | **qos** | **source** *ipv6-address*[*/ipv6-prefix*] | **sw-installed** [**non-static** | **static**]]

show mls netflow ipv6 detail [**module** *number* | **nowrap** [**module** *number*]]

show mls netflow ipv6 dynamic [**count** [**module** *number*]] [**detail**] [**module** *number*] [**nowrap** [**module** *number*]] [**qos** [**module** *number*]] [**nowrap** [**module** *number*]]

show mls netflow ipv6 flow {**icmp** | **tcp** | **udp**} [**count** [**module** *number*] | **destination** *ipv6-address*[*/ipv6-prefix*] | **detail** | **dynamic** | **flow** {**icmp** | **tcp** | **udp**} | **module** *number* | **nowrap** | **qos** | **source** *ipv6-address*[*/ipv6-prefix*] | **sw-installed** [**non-static** | **static**]]

show mls netflow ipv6 [**module** *number*]

show mls netflow ipv6 qos [**module** *number* | **nowrap** [**module** *number*]]

show mls netflow ipv6 source *ipv6-address*[*/ipv6-prefix*] [**count** [**module** *number*] | **detail** | **dynamic** | **flow** {**icmp** | **tcp** | **udp**} | **module** *number* | **nowrap** | **qos** | **sw-installed** [**non-static** | **static**]]

Syntax Description

any	Displays the NetFlow-aging information.
count	Displays the total number of Multilayer Switching (MLS) NetFlow IPv6 entries.
module *number*	(Optional) Displays the entries that are downloaded on the specified module; see the "Usage Guidelines" section for valid values.
destination *ipv6-address*	Displays the entries for a specific destination IPv6 address.
/ipv6-prefix	(Optional) IPv6 prefix; valid values are from 0 to 128.
detail	Specifies a detailed output.
dynamic	Displays the hardware-created dynamic entries.
flow {**icmp** | **tcp** | **udp**}	Specifies the flow type.
nowrap	Turns off text wrapping.
qos	Displays information about quality of service (QoS) statistics.
source *ipv6-address*	(Optional) Displays the entries for a specific source IPv6 address.
sw-installed	(Optional) Displays the routing NetFlow entries.
non-static	(Optional) Displays information about the software-installed static IPv6 entries.
static	(Optional) Displays information about the software-installed nonstatic IPv6 entries.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
12.2(17a)SX	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 to add the **show mls netflow ipv6 qos** [**module** *number*] [**nowrap**] keywords and argument on the Supervisor Engine 720 only.
12.2(18)SXF	This command was changed as follows: • Removed support for the **any** keyword. • Added the */ipv6-prefix* argument.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples This example shows how to display information about the hardware NetFlow configuration:

```
Router# show mls netflow ipv6

Displaying Netflow entries in Supervisor Earl
DstIP                                   SrcIP
---------------------------------------------------------------------------
Prot:SrcPort:DstPort   Src i/f          :AdjPtr
Pkts        Bytes       Age  LastSeen   Attributes
---------------------------------------------------------------------------------------------
50::2                                   47::2
tcp :16     :32        Vl47             :0x0
23758       1425480     4    23:48:36   L3 (IPv6) - Dynamic
50::2                                   47::3
tcp :16     :32        Vl47             :0x0
23758       1425480     4    23:48:36   L3 (IPv6) - Dynamic
50::2                                   47::4
tcp :16     :32        Vl47             :0x0
23758       1425480     4    23:48:36   L3 (IPv6) - Dynamic
50::2                                   47::5
tcp :16     :32        Vl47             :0x0
23758       1425480     4    23:48:36   L3 (IPv6) - Dynamic
50::2                                   47::6
tcp :16     :32        Vl47             :0x0
23758       1425480     4    23:48:36   L3 (IPv6) - Dynamic
```

This example shows how to display IPv6 microflow policing information:

```
Router# show mls netflow ipv6 qos

Displaying Netflow entries in Supervisor Earl
DstIP                                   SrcIP
---------------------------------------------------------------------------
Prot:SrcPort:DstPort  Src i/f          :AdjPtr    Pkts         Bytes
---------------------------------------------------------------------------
LastSeen   QoS    PoliceCount  Threshold   Leak      Drop  Bucket
---------------------------------------------------------------
101::3                                  100::2
icmp:0      :0        --               0x0          0            0
22:22:09   0x0    0                 0         0       NO  0
```

```
101::2                                  100::2
icmp:0      :0        --                0x0          0            0
22:22:09   0x0    0                  0         0       NO  0
```

This example shows how to display IPv6 microflow policing information for a specific module:

```
Router# show mls netflow ipv6 qos module 7

Displaying Netflow entries in module 7
DstIP                                   SrcIP
---------------------------------------------------------------------------
Prot:SrcPort:DstPort  Src i/f          :AdjPtr    Pkts          Bytes
---------------------------------------------------------------------------
LastSeen   QoS    PoliceCount  Threshold   Leak      Drop  Bucket
-------------------------------------------------------------------
101::2                                  100::2
icmp:0      :0        --                0x0          0            0
22:22:56   0x0    0                  0         0       NO  0
101::3                                  100::2
icmp:0      :0        --                0x0          0            0
22:22:56   0x0    0                  0         0       NO  0
```

This example shows the output display when you turn off text wrapping:

```
Router# show mls netflow ipv6 qos nowrap

Displaying Netflow entries in Supervisor Earl
DstIP                                   SrcIP
Prot:SrcPort:DstPort  Src i/f          :AdjPtr    Pkts          Bytes            LastSeen
QoS    PoliceCount  Threshold   Leak      Drop  Bucket
-------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------
-----------------------------------------------
101::3                                  100::2                                  icmp:0
:0       --             0x0        0          0            22:22:19   0x0    0
0          0       NO  0
101::2                                  100::2                                  icmp:0
:0       --             0x0        0          0            22:22:19   0x0    0
0          0       NO  0
```

This example shows the output display when you turn off text wrapping for a specific module:

```
Router# show mls netflow ipv6 qos nowrap module 7

Displaying Netflow entries in module 7
DstIP                                   SrcIP
Prot:SrcPort:DstPort  Src i/f          :AdjPtr    Pkts          Bytes            LastSeen
QoS    PoliceCount  Threshold   Leak      Drop  Bucket
-------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------
-----------------------------------------------
101::3                                  100::2                                  icmp:0
:0       --             0x0        0          0            22:22:38   0x0    0
0          0       NO  0
101::2                                  100::2                                  icmp:0
:0       --             0x0        0          0            22:22:38   0x0    0
0          0       NO  0
```

Related Commands

Command	Description
clear mls netflow	Clears the MLS NetFlow-shortcut entries.

show monitor event-trace cef ipv6

To display event trace messages for Cisco Express Forwarding IPv6 events, use the **show monitor event-trace cef ipv6** command in privileged EXEC mode.

show monitor event-trace cef ipv6 {*ipv6-address* {**all** [**detail**] | **back** {*minutes* | *hours*:*minutes*} [**detail**] | **clock** *hours*:*minutes* [*day month*] [**detail**] | **from-boot** *seconds* [**detail**] | **latest** [**detail**]} | **all** [**detail**] | **back** {*minutes* | *hours*:*minutes*} [**detail**] | **clock** *hours*:*minutes* [*day month*] [**detail**] | **from-boot** *seconds* [**detail**] | **latest** [**detail**] | **parameters**}

Syntax Description

ipv6-address	Specifies an IPv6 address. This address must be specified in hexadecimals using 16-bit values between colons, as specified in RFC 2373.
all	Displays all event trace messages currently in memory for Cisco Express Forwarding IPv6 events.
detail	(Optional) Displays detailed trace information for Cisco Express Forwarding IPv6 events.
back	Specifies how far back from the current time you want to view messages. For example, you can gather messages from the last 30 minutes.
minutes	Time argument (mmm) in minutes.
hours:*minutes*	Time argument (hh:mm) in hours and minutes. You must enter the colon (:) in the argument.
clock	Displays event trace messages starting from a specific clock time in hours and minutes format (hh:mm).
day month	(Optional) The day of the month from 1 to 31 and the name of the month of the year.
from-boot	Displays event trace messages starting after booting (uptime). To display the uptime, in seconds, enter the **show monitor event-trace cef from-boot ?** command.
seconds	(Optional) Displays event trace messages starting from a specified number of seconds after booting (uptime). Range: 0 to 3279.
latest	Displays only the event trace messages generated since the last **show monitor event-trace cef ipv6** command was entered.
parameters	Displays parameters configured for the trace.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.
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 the **show monitor event-trace cef ipv6** command to display trace message information for Cisco Express Forwarding IPv6 events.

The trace function is not locked while information is displayed to the console. This means that new trace messages can accumulate in memory. If entries accumulate faster than they can be displayed, some messages can be lost. If this happens, the **show monitor event-trace cef ipv6** command generates a message indicating that some messages might be lost; however, messages continue to be displayed on the console. If the number of lost messages is excessive, the **show monitor event-trace cef ipv6** command stops displaying messages.

Examples

The following is a sample of the **show monitor event-trace cef ipv6 all** command:

```
Router# show monitor event-trace cef ipv6 all

*Aug 22 20:14:59.075:  [Default] *::*/*                Allocated FIB table
                      [OK]
*Aug 22 20:14:59.075:  [Default] *::*/*'00             Add source Default table
                      [OK]
*Aug 22 20:14:59.075:  [Default] ::/0'00               FIB add src DRH (ins)
                      [OK]
*Aug 22 20:14:59.075:  [Default] *::*/*'00             New FIB table
                      [OK]
```

Table 284 describes the significant fields shown in the display.

Table 284 show monitor event-trace cef ipv6 all Field Descriptions

Field	Description
*Aug 22 20:14:59.075:	Time stamp that indicates the month, day, and time when the event was captured.
[Default] *::*/*	Identifies the default VRF.
Allocated FIB table [OK]	Provides the event detail and indicates if the event happened. In this instance, a FIB table was allocated.

The following is sample output from the **show monitor event-trace cef ipv6 parameters** command:

```
Router# show monitor event-trace cef ipv6 parameters

Trace has 1000 entries
Stacktrace is disabled by default
Matching all events
```

Table 285 describes the significant fields shown in the display.

Table 285 show monitor event-trace cef ipv6 parameters Field Descriptions

Field	Description
Trace has 1000 entries	The size of the event logging buffer is 1000 entries.
Stacktrace is disabled by default	Stack trace at tracepoints is disabled.
Matching all events	Event tracing for all events is matched.

Related Commands

Command	Description
monitor event-trace cef (EXEC)	Monitors and controls the event trace function for Cisco Express Forwarding.
monitor event-trace cef (global)	Configures event tracing for Cisco Express Forwarding.
monitor event-trace cef ipv4 (global)	Configures event tracing for Cisco Express Forwarding IPv4 events.
monitor event-trace cef ipv6 (global)	Configures event tracing for Cisco Express Forwarding IPv6 events.
show monitor event-trace cef	Displays event trace messages for Cisco Express Forwarding.
show monitor event-trace cef events	Displays event trace messages for Cisco Express Forwarding events.
show monitor event-trace cef interface	Displays event trace messages for Cisco Express Forwarding interface events.
show monitor event-trace cef ipv4	Displays event trace messages for Cisco Express Forwarding IPv4 events.

show monitor event-trace vpn-mapper

To display event trace messages for IPv6 virtual private networks (VPNs), use the **show monitor event-trace vpn-mapper** command in privileged EXEC mode.

show monitor event-trace vpn-mapper {**latest** | **all**}

Syntax Description

latest	Displays only the event trace messages since the last **show monitor event-trace** command was entered.
all	Displays all event trace messages currently in memory for the specified component.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(33)SRB1	This command was introduced.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Use the **show monitor event-trace** command to display trace message information about IPv6 VPNs.

Examples

The following example allows event trace messages for IPv6 VPNs to be displayed:

```
Router# show monitor event-trace vpn-mapper
```

show mpls forwarding-table

To display the contents of the Multiprotocol Label Switching (MPLS) Label Forwarding Information Base (LFIB), use the **show mpls forwarding-table** command in user EXEC or privileged EXEC mode.

show mpls forwarding-table [*network* {*mask* | *length*} | **interface** *interface* | **labels** *label* [**-** *label*] | **lcatm atm** *atm-interface-number* | **next-hop** *address* | **lsp-tunnel** [*tunnel-id*]] [**vrf** *vrf-name*] [**detail slot** *slot-number*]

Syntax Description

network	(Optional) Destination network number.
mask	IP address of the destination mask whose entry is to be shown.
length	Number of bits in the mask of the destination.
interface *interface*	(Optional) Displays entries with the outgoing interface specified.
labels *label - label*	(Optional) Displays entries with the local labels specified.
lcatm atm *atm-interface-number*	Displays ATM entries with the specified Label Controlled Asynchronous Transfer Mode (LCATM).
next-hop *address*	(Optional) Displays only entries with the specified neighbor as the next hop.
lsp-tunnel	(Optional) Displays only entries with the specified label switched path (LSP) tunnel, or with all LSP tunnel entries.
tunnel-id	(Optional) Specifies the LSP tunnel for which to display entries.
vrf *vrf-name*	(Optional) Displays entries with the specified VPN routing and forwarding (VRF) instance.
detail	(Optional) Displays information in long form (includes length of encapsulation, length of MAC string, maximum transmission unit [MTU], and all labels).
slot *slot-number*	(Optional) Specifies the slot number, which is always 0.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
11.1CT	This command was introduced.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T. The command was updated with MPLS terminology and command syntax.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. The command was modified to accommodate use of the MPLS experimental (EXP) level as a selection criterion for packet forwarding. The output display was modified to include a bundle adjacency field and exp (vcd) values when the optional **detail** keyword is specified.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S. The IPv6 MPLS aggregate label and prefix information was added to the display.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.

Release	Modification
12.0(27)S	This command was integrated into Cisco IOS Release 12.0(27)S. The command output was modified to include explicit-null label information.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S. The output was changed in the following ways: • The term "tag" was replaced with the term "label." • The term "untagged" was replaced with the term "no label."
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA. This command was modified to remove the **lsp-tunnel** keyword.
12.2(33)SXH	This command was modified. The command output shows the status of local labels in holddown for the Cisco IOS Software Modularity: MPLS Layer 3 VPNs feature. The status indicator showing that traffic is forwarded through an LSP tunnel is moved to the local label and the **lsp-tunnel** keyword was removed.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.
15.1(1)S	This command was integrated into Cisco IOS Release 15.1(1)S. The output was modified to display the pseudowire identifier when the **interface** keyword is used.

Examples

The following is sample output from the **show mpls forwarding-table** command:

```
Router# show mpls forwarding-table

Local Outgoing      Prefix            Bytes label Outgoing       Next Hop
Label Label or VC   or Tunnel Id      switched  interface
26    No Label      10.253.0.0/16     0         Et4/0/0       10.27.32.4
28    1/33          10.15.0.0/16      0         AT0/0.1       point2point
29    Pop Label     10.91.0.0/16      0         Hs5/0         point2point
      1/36          10.91.0.0/16      0         AT0/0.1       point2point
30    32            10.250.0.97/32    0         Et4/0/2       10.92.0.7
      32            10.250.0.97/32    0         Hs5/0         point2point
34    26            10.77.0.0/24      0         Et4/0/2       10.92.0.7
      26            10.77.0.0/24      0         Hs5/0         point2point
35    No Label[T]   10.100.100.101/32 0         Tu301         point2point
36    Pop Label     10.1.0.0/16       0         Hs5/0         point2point
      1/37          10.1.0.0/16       0         AT0/0.1       point2point

[T]     Forwarding through a TSP tunnel.
        View additional labeling info with the 'detail' option
```

The following is sample output from the **show mpls forwarding-table** command when the IPv6 Provider Edge Router over MPLS feature is configured to allow IPv6 traffic to be transported across an IPv4 MPLS backbone. The labels are aggregated because there are several prefixes for one local label, and the prefix column contains "IPv6" instead of a target prefix.

```
Router# show mpls forwarding-table

Local Outgoing      Prefix            Bytes label Outgoing       Next Hop
Label Label or VC   or Tunnel Id      switched  interface
16    Aggregate     IPv6              0
17    Aggregate     IPv6              0
18    Aggregate     IPv6              0
19    Pop Label     192.168.99.64/30  0         Se0/0         point2point
```

```
20    Pop Label     192.168.99.70/32  0         Se0/0         point2point
21    Pop Label     192.168.99.200/32 0         Se0/0         point2point
22    Aggregate     IPv6              5424
23    Aggregate     IPv6              3576
24    Aggregate     IPv6              2600
```

The following is sample output from the **show mpls forwarding-table** command when you specify the **detail** keyword. If the MPLS EXP level is used as a selection criterion for packet forwarding, a bundle adjacency exp (vcd) field is included in the display. This field includes the EXP value and the corresponding virtual circuit descriptor (VCD) in parentheses. The line in the output that reads "No output feature configured" indicates that the MPLS egress NetFlow accounting feature is not enabled on the outgoing interface for this prefix.

```
Router# show mpls forwarding-table detail

Local Outgoing      Prefix            Bytes label Outgoing       Next Hop
label   label or VC     or Tunnel Id      switched  interface
16    Pop label       10.0.0.6/32        0         AT1/0.1       point2point
      Bundle adjacency exp(vcd)
      0(1) 1(1) 2(1) 3(1) 4(1) 5(1) 6(1) 7(1)
      MAC/Encaps=12/12, MTU=4474, label Stack{}
      00010000AAAA030000008847
      No output feature configured
17    18            10.0.0.9/32        0         AT1/0.1       point2point
      Bundle adjacency exp(vcd)
      0(1) 1(1) 2(1) 3(1) 4(1) 5(1) 6(1) 7(1)
      MAC/Encaps=12/16, MTU=4470, label Stack{18}
      00010000AAAA030000008847 00012000
      No output feature configured
18    19            10.0.0.10/32        0        AT1/0.1       point2point
      Bundle adjacency exp(vcd)
      0(1) 1(1) 2(1) 3(1) 4(1) 5(1) 6(1) 7(1)
      MAC/Encaps=12/16, MTU=4470, label Stack{19}
      00010000AAAA030000008847 00013000
      No output feature configured
19    17            10.0.0.0/8         0        AT1/0.1       point2point
      Bundle adjacency exp(vcd)
      0(1) 1(1) 2(1) 3(1) 4(1) 5(1) 6(1) 7(1)
      MAC/Encaps=12/16, MTU=4470, label Stack{17}
      00010000AAAA030000008847 00011000
      No output feature configured
20    20            10.0.0.0/8         0        AT1/0.1       point2point
      Bundle adjacency exp(vcd)
      0(1) 1(1) 2(1) 3(1) 4(1) 5(1) 6(1) 7(1)
      MAC/Encaps=12/16, MTU=4470, label Stack{20}
      00010000AAAA030000008847 00014000
      No output feature configured
21    Pop label       10.0.0.0/24        0        AT1/0.1       point2point
      Bundle adjacency exp(vcd)
      0(1) 1(1) 2(1) 3(1) 4(1) 5(1) 6(1) 7(1)
      MAC/Encaps=12/12, MTU=4474, label Stack{}
      00010000AAAA030000008847
      No output feature configured
22    Pop label       10.0.0.4/32         0        Et2/3         10.0.0.4
      MAC/Encaps=14/14, MTU=1504, label Stack{}
      000427AD10430005DDFE043B8847
      No output feature configured
```

The following is sample output from the **show mpls forwarding-table** command when you use the **detail** keyword. In this example, the MPLS egress NetFlow accounting feature is enabled on the first three prefixes, as indicated by the line in the output that reads "Feature Quick flag set."

```
Router# show mpls forwarding-table detail

Local  Outgoing    Prefix            Bytes label  Outgoing   Next Hop
label    label or VC   or Tunnel Id      switched   interface
16     Aggregate   10.0.0.0/8[V]     0
        MAC/Encaps=0/0, MTU=0, label Stack{}
        VPN route: vpn1
        Feature Quick flag set
Per-packet load-sharing, slots: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
17     No label    10.0.0.0/8[V]      0          Et0/0/2    10.0.0.1
        MAC/Encaps=0/0, MTU=1500, label Stack{}
        VPN route: vpn1
        Feature Quick flag set
Per-packet load-sharing, slots: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
18     No label    10.42.42.42/32[V] 4185       Et0/0/2    10.0.0.1
        MAC/Encaps=0/0, MTU=1500, label Stack{}
        VPN route: vpn1
        Feature Quick flag set
Per-packet load-sharing, slots: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
19     2/33        10.41.41.41/32    0          AT1/0/0.1  point2point
        MAC/Encaps=4/8, MTU=4470, label Stack{2/33(vcd=2)}
        00028847 00002000
        No output feature configured
```

Cisco 10000 Series Examples

The following is sample output from the **show mpls forwarding-table** command for Cisco 10000 series routers:

```
Router# show mpls forwarding-table

Local   Outgoing      Prefix            Bytes Label   Outgoing   Next Hop
Label   Label or VC   or Tunnel Id      Switched      interface
16      Pop Label     10.0.0.0/8        0             Fa1/0/0    10.0.0.2
        Pop Label     10.0.0.0/8        0             Fa1/1/0    10.0.0.2
17      Aggregate     10.0.0.0/8[V]     570           vpn2
21      Pop Label     10.11.11.11/32    0             Fa1/0/0    10.0.0.2
22      Pop Label     10.12.12.12/32    0             Fa1/1/0    10.0.0.2
23      No Label      10.3.0.0/16[V]     0             Fa4/1/0   10.0.0.2
```

The following is sample output from the **show mpls forwarding-table** command when you specify the **detail** keyword for Cisco 10000 series routers:

```
Router# show mpls forwarding-table detail

Local   Outgoing      Prefix            Bytes Label   Outgoing   Next Hop
Label   Label or VC   or Tunnel Id      Switched      interface
16      Pop Label     10.0.0.0/8        0             Fa1/0/0    10.0.0.2
        MAC/Encaps=14/14, MRU=1500, Label Stack{}
        000B45C93889000B45C930218847
        No output feature configured
        Pop Label     10.0.0.0/8        0             Fa1/1/0     10.0.0.2
        MAC/Encaps=14/14, MRU=1500, Label Stack{}
        000B45C92881000B45C930288847
        No output feature configured
17      Aggregate    10.0.0.0/8[V]      570           vpn2
        MAC/Encaps=0/0, MRU=0, Label Stack{}
        VPN route: vpn2
        No output feature configured
21      Pop Label     10.11.11.11/32     0            Fa1/0/0     10.0.0.2
```

```
 MAC/Encaps=14/14, MRU=1500, Label Stack{}
000B45C93889000B45C930218847
No output feature configured
```

Table 286 describes the significant fields shown in the displays.

Table 286 show mpls forwarding-table Field Descriptions

Field	Description
Local label	Label assigned by this router.
Outgoing Label or VC **Note** This field is not supported on the Cisco 10000 series routers.	Label assigned by the next hop or the virtual path identifier (VPI)/virtual channel identifier (VCI) used to get to next hop. The entries in this column are the following: • [T]—Forwarding is through an LSP tunnel. • No Label—There is no label for the destination from the next hop or label switching is not enabled on the outgoing interface. • Pop Label—The next hop advertised an implicit NULL label for the destination and the router removed the top label. • Aggregate—There are several prefixes for one local label. This entry is used when IPv6 is configured on edge routers to transport IPv6 traffic over an IPv4 MPLS network.
Prefix or Tunnel Id	Address or tunnel to which packets with this label are sent. **Note** If IPv6 is configured on edge routers to transport IPv6 traffic over an IPv4 MPLS network, “IPv6” is displayed here. • [V]—The corresponding prefix is in a VRF.
Bytes label switched	Number of bytes switched with this incoming label. This includes the outgoing label and Layer 2 header.
Outgoing interface	Interface through which packets with this label are sent.
Next Hop	IP address of the neighbor that assigned the outgoing label.
Bundle adjacency exp(vcd)	Bundle adjacency information. Includes the MPLS EXP value and the corresponding VCD.
MAC/Encaps	Length in bytes of the Layer 2 header and length in bytes of the packet encapsulation, including the Layer 2 header and label header.
MTU	MTU of the labeled packet.
label Stack	All the outgoing labels. If the outgoing interface is transmission convergence (TC)-ATM, the VCD is also shown. **Note** TC-ATM is not supported on Cisco 10000 series routers.
00010000AAAA030000008847 00013000	The actual encapsulation in hexadecimal form. A space is shown between Layer 2 and the label header.

Explicit-Null Label Example

The following is sample output, including the explicit-null label = 0 (commented in bold), for the **show mpls forwarding-table** command on a CSC-PE router:

```
Router# show mpls forwarding-table

Local  Outgoing      Prefix            Bytes label  Outgoing   Next Hop
label  label or VC   or Tunnel Id      switched     interface
17     Pop label     10.10.0.0/32      0            Et2/0      10.10.0.1
18     Pop label     10.10.10.0/24     0            Et2/0      10.10.0.1
19     Aggregate     10.10.20.0/24[V]  0
20     Pop label     10.10.200.1/32[V] 0            Et2/1      10.10.10.1
21     Aggregate     10.10.1.1/32[V]   0
22     0             192.168.101.101/32[V]   \
                                       0            Et2/1      192.168.101.101
23     0             192.168.101.100/32[V]   \
                                       0            Et2/1      192.168.101.100
25     0             192.168.102.125/32[V] 0        Et2/1      192.168.102.125 !outlabel
value 0
```

Table 287 describes the significant fields shown in the display.

Table 287 show mpls forwarding-table Field Descriptions

Field	Description
Local label	Label assigned by this router.
Outgoing label or VC	Label assigned by the next hop or VPI/VCI used to get to the next hop. The entries in this column are the following: • [T]—Forwarding is through an LSP tunnel. • No label—There is no label for the destination from the next hop or that label switching is not enabled on the outgoing interface. • Pop label—The next hop advertised an implicit NULL label for the destination and that this router popped the top label. • Aggregate—There are several prefixes for one local label. This entry is used when IPv6 is configured on edge routers to transport IPv6 traffic over an IPv4 MPLS network. • 0—The explicit null label value = 0.
Prefix or Tunnel Id	Address or tunnel to which packets with this label are sent. **Note** If IPv6 is configured on edge routers to transport IPv6 traffic over an IPv4 MPLS network, IPv6 is displayed here. • [V]—Means that the corresponding prefix is in a VRF.
Bytes label switched	Number of bytes switched with this incoming label. This includes the outgoing label and Layer 2 header.
Outgoing interface	Interface through which packets with this label are sent.
Next Hop	IP address of the neighbor that assigned the outgoing label.

Cisco IOS Software Modularity: MPLS Layer 3 VPNs Example

The following is sample output from the **show mpls forwarding-table** command:

```
Router# show mpls forwarding-table

Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
16         Pop Label  IPv4 VRF[V]      62951000      aggregate/v1
17    [H]  No Label   10.1.1.0/24      0             AT1/0/0.1 point2point
           No Label   10.1.1.0/24      0             PO3/1/0 point2point
      [T]  No Label   10.1.1.0/24      0             Tu1 point2point
18    [HT] Pop Label  10.0.0.3/32      0             Tu1 point2point
19    [H]  No Label   10.0.0.0/8       0             AT1/0/0.1 point2point
           No Label   10.0.0.0/8       0             PO3/1/0 point2point
20    [H]  No Label   10.0.0.0/8       0             AT1/0/0.1 point2point
           No Label   10.0.0.0/8       0             PO3/1/0 point2point
21    [H]  No Label   10.0.0.1/32      812           AT1/0/0.1 point2point
           No Label   10.0.0.1/32      0             PO3/1/0 point2point
22    [H]  No Label   10.1.14.0/24     0             AT1/0/0.1 point2point
           No Label   10.1.14.0/24     0             PO3/1/0 point2point
23    [HT] 16         172.1.1.0/24[V]  0             Tu1 point2point
24    [HT] 24         10.0.0.1/32[V]   0             Tu1 point2point
25    [H]  No Label   10.0.0.0/8[V]    0             AT1/1/0.1 point2point
26    [HT] 16         10.0.0.3/32[V]   0             Tu1 point2point
27         No Label   10.0.0.1/32[V]   0             AT1/1/0.1 point2point

[T]     Forwarding through a TSP tunnel.
        View additional labelling info with the 'detail' option
[H]     Local label is being held down temporarily.
```

Table 288 describes the Local Label fields relating to the Cisco IOS Software Modularity: MPLS Layer 3 VPNs feature.

Table 288 show mpls forwarding-table Field Descriptions

Field	Description
Local Label	Label assigned by this router. • [H]—Local labels are in holddown, which means that the application that requested the labels no longer needs them and stops advertising them to its labeling peers. The label's forwarding-table entry is deleted after a short, application-specific time. If any application starts advertising a held-down label to its labeling peers, the label could come out of holddown. **Note** [H] is not shown if labels are held down globally. A label enters global holddown after a stateful switchover or a restart of certain processes in a Cisco IOS modularity environment. • [T]—The label is forwarded through an LSP tunnel. **Note** Although [T] is still a property of the outgoing interface, it is shown in the Local Label column. • [HT]—Both conditions apply.

L2VPN Inter-AS Option B: Example

The following is sample output from the **show mpls forwarding-table interface** command. In this example, the pseudowire identifier (that is, 4096) is displayed in the Prefix or Tunel Id column. The **show mpls l2transport vc detail** command can be used to obtain more information about the specific pseudowire displayed.

```
Router# show mpls forwarding-table

Local      Outgoing   Prefix           Bytes Label    Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched       interface
1011       No Label   l2ckt(4096)          0          none       point2point
```

Table 289 describes the fields shown in the display.

Table 289 show mpls forwarding-table interface Field Descriptions

Field	Description
Local Label	Label assigned by this router.
Outgoing Label	Label assigned by the next hop or virtual path identifier (VPI)/virtual channel identifier (VCI) used to get to the next hop.
Prefix or Tunnel Id	Address or tunnel to which packets with this label are going.
Bytes Label Switched	Number of bytes switched with this incoming label. This includes the outgoing label and Layer 2 header.

Table 289 show mpls forwarding-table interface Field Descriptions (continued)

Field	Description
Outgoing interface	Interface through which packets with this label are sent.
Next Hop	IP address of the neighbor that assigned the outgoing label.

Related Commands

Command	Description
neighbor send-label	Enables a BGP router to send MPLS labels with BGP routes to a neighboring BGP router.
neighbor send-label explicit-null	Enables a BGP router to send MPLS labels with explicit-null information for a CSC-CE router and BGP routes to a neighboring CSC-PE router.
show mpls l2transport vc detail	Displays information about AToM VCs and static pseudowires that have been enabled to route Layer 2 packets on a router.

show ntp associations

To display the status of Network Time Protocol (NTP) associations, use the **show ntp associations** command in user EXEC or privileged EXEC mode.

show ntp associations [**detail**]

Syntax Description

detail	(Optional) Displays detailed information about each NTP association.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(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 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.

Examples

Detailed descriptions of the information displayed by this command can be found in the NTP specification (RFC 1305).

The following is sample output from the **show ntp associations** command:

```
Router> show ntp associations

     address         ref clock     st  when  poll  reach  delay  offset    disp
 ~172.31.32.2      172.31.32.1       5    29  1024  377     4.2   -8.59     1.6
+~192.168.13.33    192.168.1.111     3    69   128  377     4.1    3.48     2.3
*~192.168.13.57    192.168.1.111     3    32   128  377     7.9   11.18     3.6
* master (synced), # master (unsynced), + selected, - candidate, ~ configured
```

Table 290 describes the significant fields shown in the display.

Table 290 show ntp associations Field Descriptions

Field	Description
address	Address of the peer.
ref clock	Address of the reference clock of the peer.
st	Stratum of the peer.
when	Time since the last NTP packet was received from the peer (in seconds).

Table 290 show ntp associations Field Descriptions (continued)

Field	Description
poll	Polling interval (in seconds).
reach	Peer reachability (bit string, in octal).
delay	Round-trip delay to the peer (in milliseconds).
offset	Relative time of the peer clock to the local clock (in milliseconds).
disp	Dispersion.
*	Synchronized to this peer.
#	Almost synchronized to this peer.
+	Peer selected for possible synchronization.
-	Peer is a candidate for selection.
~	Peer is statically configured.

The following is sample output from the **show ntp associations detail** command:

```
Router> show ntp associations detail

172.31.32.2 configured, insane, invalid, stratum 5
ref ID 172.31.32.1, time AFE252C1.6DBDDFF2 (00:12:01.428 PDT Mon Jul 5 1993)
our mode active, peer mode active, our poll intvl 1024, peer poll intvl 64
root delay 137.77 msec, root disp 142.75, reach 376, sync dist 215.363
delay 4.23 msec, offset -8.587 msec, dispersion 1.62
precision 2**19, version 3
org time AFE252E2.3AC0E887 (00:12:34.229 PDT Mon Jul 5 1993)
rcv time AFE252E2.3D7E464D (00:12:34.240 PDT Mon Jul 5 1993)
xmt time AFE25301.6F83E753 (00:13:05.435 PDT Mon Jul 5 1993)
filtdelay =     4.23    4.14    2.41    5.95    2.37    2.33    4.26    4.33
filtoffset =   -8.59   -8.82   -9.91   -8.42  -10.51  -10.77  -10.13  -10.11
filterror =     0.50    1.48    2.46    3.43    4.41    5.39    6.36    7.34

192.168.13.33 configured, selected, sane, valid, stratum 3
ref ID 192.168.1.111, time AFE24F0E.14283000 (23:56:14.078 PDT Sun Jul 4 1993)
our mode client, peer mode server, our poll intvl 128, peer poll intvl 128
root delay 83.72 msec, root disp 217.77, reach 377, sync dist 264.633
delay 4.07 msec, offset 3.483 msec, dispersion 2.33
precision 2**6, version 3
org time AFE252B9.713E9000 (00:11:53.442 PDT Mon Jul 5 1993)
rcv time AFE252B9.7124E14A (00:11:53.441 PDT Mon Jul 5 1993)
xmt time AFE252B9.6F625195 (00:11:53.435 PDT Mon Jul 5 1993)
filtdelay =     6.47    4.07    3.94    3.86    7.31    7.20    9.52    8.71
filtoffset =    3.63    3.48    3.06    2.82    4.51    4.57    4.28    4.59
filterror =     0.00    1.95    3.91    4.88    5.84    6.82    7.80    8.77

192.168.13.57 configured, our_master, sane, valid, stratum 3
ref ID 192.168.1.111, time AFE252DC.1F2B3000 (00:12:28.121 PDT Mon Jul 5 1993)
our mode client, peer mode server, our poll intvl 128, peer poll intvl 128
root delay 125.50 msec, root disp 115.80, reach 377, sync dist 186.157
delay 7.86 msec, offset 11.176 msec, dispersion 3.62
precision 2**6, version 2
org time AFE252DE.77C29000 (00:12:30.467 PDT Mon Jul 5 1993)
rcv time AFE252DE.7B2AE40B (00:12:30.481 PDT Mon Jul 5 1993)
xmt time AFE252DE.6E6D12E4 (00:12:30.431 PDT Mon Jul 5 1993)
filtdelay =    49.21    7.86    8.18    8.80    4.30    4.24    7.58    6.42
filtoffset =   11.30   11.18   11.13   11.28    8.91    9.09    9.27    9.57
```

```
filterror =     0.00    1.95    3.91    4.88    5.78    6.76    7.74    8.71
```

Table 291 describes the significant fields shown in the display.

Table 291 show ntp associations detail Field Descriptions

Field	Descriptions
configured	Peer was statically configured.
insane	Peer fails basic checks.
invalid	Peer time is believed to be invalid.
ref ID	Address of the machine the peer is synchronized to.
time	Last time stamp the peer received from its master.
our mode	Mode of the source relative to the peer (active/passive/client/server/bdcast/bdcast client).
peer mode	Peer's mode relative to the source.
our poll intvl	Source poll interval to the peer.
peer poll intvl	Peer's poll interval to the source.
root delay	Delay (in milliseconds) along the path to the root (ultimate stratum 1 time source).
root disp	Dispersion of the path to the root.
reach	Peer reachability (bit string in octal).
sync dist	Peer synchronization distance.
delay	Round-trip delay to the peer (in milliseconds).
offset	Offset of the peer clock relative to the system clock.
dispersion	Dispersion of the peer clock.
precision	Precision of the peer clock in Hertz.
version	NTP version number that the peer is using.
org time	Originate time stamp.
rcv time	Receive time stamp.
xmt time	Transmit time stamp.
filtdelay	Round-trip delay (in milliseconds) of each sample.
filtoffset	Clock offset (in milliseconds) of each sample.
filterror	Approximate error of each sample.
sane	Peer passes basic checks.
selected	Peer is selected for possible synchronization.
valid	Peer time is believed to be valid.
our_master	Local machine is synchronized to this peer.

Related Commands

Command	Description
show ntp status	Displays the status of the NTP.

show ntp status

To display the status of the Network Time Protocol (NTP), use the **show ntp status** command in user EXEC or privileged EXEC mode.

show ntp status

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(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 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.

Examples

The following is sample output from the **show ntp status** command:

```
Router> show ntp status

Clock is synchronized, stratum 4, reference is 192.168.13.57
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**19
reference time is AFE2525E.70597B34 (00:10:22.438 PDT Mon Jul 5 1993)
clock offset is 7.33 msec, root delay is 133.36 msec
root dispersion is 126.28 msec, peer dispersion is 5.98 msec
```

Table 292 describes the significant fields shown in the display.

Table 292 show ntp status Field Descriptions

Field	Description
synchronized	System is synchronized to an NTP peer.
stratum	NTP stratum of this system.
reference	Address of the peer the system is synchronized to.
nominal freq	Nominal frequency of the system hardware clock (in Hertz).
actual freq	Measured frequency of the system hardware clock (in Hertz).
precision	Precision of the clock of this system (in Hertz).

Table 292 show ntp status Field Descriptions (continued)

Field	Description
reference time	Reference time stamp.
clock offset	Offset of the system clock to the synchronized peer (in milliseconds).
root delay	Total delay along the path to the root clock (in milliseconds).
root dispersion	Dispersion of the root path.
peer dispersion	Dispersion of the synchronized peer.

Related Commands

Command	Description
show ntp associations	Displays the status of the NTP associations.

show ospfv3 border-routers

To display the internal Open Shortest Path First version 3 (OSPFv3) routing table entries to an Area Border Router (ABR) and Autonomous System Boundary Router (ASBR), use the **show ospfv3 border-routers** command in privileged EXEC mode.

show ospfv3 [*process-id*] [*address-family*] **border-routers**

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Examples

The following examples enables the display of the internal OSPFv3 routing table entries to an ABR and ASBR:

```
Router# show ospfv3 border-routers
```

show ospfv3 database

To display lists of information related to the Open Shortest Path First version 3 (OSPFv3) database for a specific router, use the **show ospfv3 database** command in user EXEC or privileged EXEC mode. The various forms of this command deliver information about different OSPFv3 link-state advertisements (LSAs).

show ospfv3 [*process-id* [*area-id*]] [*address-family*] **database** [**database-summary** | **internal** | **external** [*ipv6-prefix*] [*link-state-id*] | **grace** | **inter-area prefix** [*ipv6-prefix* | *link-state-id*] | **inter-area router** [*destination-router-id* | *link-state-id*] | **link** [**interface** *interface-name* | *link-state-id*] | **network** [*link-state-id*] | **nssa-external** [*ipv6-prefix*] [*link-state-id*] | **prefix** [**ref-lsa** {**router** | **network**} | *link-state-id*] | **promiscuous** | **router** [*link-state-id*] | **unknown** [{**area** | **as** | **link**} [*link-state-id*]] [**adv-router** *router-id*] [**self-originate**]

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
area-id	(Optional) Displays information only about a specified area. The *area-id* argument can only be used if the *process-id* argument is specified.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
database-summary	(Optional) Displays how many of each type of LSAs exist for each area in the database, and the total.
internal	(Optional) Internal LSA information.
external	(Optional) Displays information only about the external LSAs.
ipv6-prefix	(Optional) Link-local IPv6 address of the neighbor. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
grace	(Optional) Displays information about OSPFv3 graceful restart.
link-state-id	(Optional) An integer used to differentiate LSAs. In network and link LSAs, the link-state ID matches the interface index.
inter-area prefix	(Optional) Displays information only about LSAs based on inter-area prefix LSAs.
inter-area router	(Optional) Displays information only about LSAs based on inter-area router LSAs.
destination-router-id	(Optional) The specified destination router ID.
link	(Optional) Displays information about the link LSAs.
interface	(Optional) Displays information about the LSAs filtered by interface context.
interface-name	(Optional) Specifies the LSA interface.
network	(Optional) Displays information only about the network LSAs.
nssa-external	(Optional) Displays information only about the not so stubby area (NSSA) external LSAs.
prefix	(Optional) Displays information on the intra-area-prefix LSAs.

promiscuous	(Optional) Displays temporary LSAs in a Mobile Ad Hoc Network (MANET).
ref-lsa {**router** | **network**}	(Optional) Further filters the prefix LSA type.
router	(Optional) Displays information only about the router LSAs.
unknown	(Optional) Displays all LSAs with unknown types.
area	(Optional) Filters unknown area LSAs.
as	(Optional) Filters unknown autonomous system (AS) LSAs.
link	(Optional) When following the **unknown** keyword, the **link** keyword filters link-scope LSAs.
adv-router *router-id*	(Optional) Displays all the LSAs of the advertising router. This argument must be in the form documented in RFC 2740 where the address is specified in hexadecimal using 16-bit values between colons.
self-originate	(Optional) Displays only self-originated LSAs (from the local router).

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

The **adv-router** keyword requires a router ID. The **self-originate** keyword displays only those LSAs that originated from the local router. Both of these keywords can be appended to all other keywords used with the **show ospfv3 database** database command to provide more detailed information.

Examples

The following is sample output from the **show ospfv3 database** command when no arguments or keywords are used:

```
Router# show ospfv3 database

            OSPFv3 Router with ID (172.16.4.4) (Process ID 1)

                Router Link States (Area 0)

ADV Router         Age         Seq#        Fragment ID   Link count  Bits
172.16.4.4         239         0x80000003  0             1           B
172.16.6.6         239         0x80000003  0             1           B

            Inter Area Prefix Link States (Area 0)

ADV Router         Age         Seq#        Prefix
172.16.4.4         249         0x80000001  FEC0:3344::/32
172.16.4.4         219         0x80000001  FEC0:3366::/32
172.16.6.6         247         0x80000001  FEC0:3366::/32
```

```
172.16.6.6         193         0x80000001  FEC0:3344::/32
172.16.6.6         82          0x80000001  FEC0::/32

            Inter Area Router Link States (Area 0)

ADV Router         Age         Seq#        Link ID    Dest RtrID
172.16.4.4         219         0x80000001  50529027   172.16.3.3
172.16.6.6         193         0x80000001  50529027   172.16.3.3

            Link (Type-8) Link States (Area 0)

ADV Router         Age         Seq#        Link ID    Interface
172.16.4.4         242         0x80000002  14         PO4/0
172.16.6.6         252         0x80000002  14         PO4/0

            Intra Area Prefix Link States (Area 0)

ADV Router         Age         Seq#        Link ID    Ref-lstype  Ref-LSID
172.16.4.4         242         0x80000002  0          0x2001      0
172.16.6.6         252         0x80000002  0          0x2001      0
```

Table 293 describes the significant fields shown in the display.

Table 293 show ospfv3 database Field Descriptions

Field	Description
ADV Router	Advertising router ID.
Age	Link-state age.
Seq#	Link-state sequence number (detects old or duplicate LSAs).
Link ID	Interface ID number.
Ref-lstype	Referenced link-state type.
Ref-LSID	Referenced link-state ID.

show ospfv3 events

To display detailed information about Open Shortest Path First version 3 (OSPFv3) events, use the **show ospfv3 events** command in privileged EXEC mode.

show ospfv3 [*process-id*] [*address-family*] **events** [**generic** | **interface** | **lsa** | **neighbor** | **reverse** | **rib** | **spf**]

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
generic	(Optional) Generic information regarding OSPFv3 events.
interface	(Optional) Interface state change events, including old and new states.
lsa	(Optional) LSA arrival and LSA generation events.
neighbor	(Optional) Neighbor state change events, including old and new states.
reverse	(Optional) Keyword to allow the display of events in reverse–from the latest to the oldest or from oldest to the latest.
rib	(Optional) Routing Information Base (RIB) update, delete, and redistribution events.
spf	(Optional) Scheduling and SPF run events.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

An OSPFv3 event log is kept for every OSPFv3 instance. If you enter the **show ospfv3 events** command without any keywords, all information in the OSPFv3 event log is displayed. Use the keywords to filter specific information.

Examples

The following example enables the display of information about OSPFv3 events:

```
Router# show ospfv3 events
```

show ospfv3 flood-list

To display a list of Open Shortest Path First version 3 (OSPFv3) link-state advertisements (LSAs) waiting to be flooded over an interface, use the **show ospfv3 flood-list** command in privileged EXEC mode.

show ospfv3 [*process-id*] [*area-id*] [*address-family*] **flood-list** *interface-type interface-number*

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
area-id	(Optional) Displays information only about a specified area.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
interface-type	Interface type over which the LSAs will be flooded.
interface-number	Interface number over which the LSAs will be flooded.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

Use this command to display OSPFv3 packet pacing.

Examples

The following displays a list of OSPFv3 LSAs waiting to be flooded over an interface:

```
Router# show ospfv3 flood-list
```

show ospfv3 graceful-restart

To display Open Shortest Path First version 3 (OSPFv3) graceful restart information, use the **show ospfv3 graceful-restart** command in privileged EXEC mode.

show ospfv3 [*process-id*] [*address-family*] **graceful-restart**

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

Use the **show ospfv3 graceful-restart** command to discover information about the OSPFv3 graceful restart feature.

Examples

The following example displays OSPFv3 graceful restart information :

```
Router# show ospfv3 graceful-restart
```

show ospfv3 interface

To display Open Shortest Path First version 3 (OSPFv3)-related interface information, use the **show ospfv3 interface** command in privileged mode.

show ospfv3 [*process-id*] [*area-id*] [*address-family*] **interface** [*type number*] [**brief**]

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
area-id	(Optional) Displays information about a specified area only.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
type number	(Optional) Interface type and number.
brief	(Optional) Displays brief overview information for OSPFv3 interfaces, states, addresses and masks, and areas on the router.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Examples

The following is sample output from the **show ospfv3 interface** command for a Mobile Ad Hoc Network (MANET) environment:

```
Router# show ospfv3 interface

Ethernet0/0 is up, line protocol is up
 Link Local Address FE80::A8BB:CCFF:FE01:5500, Interface ID 3
 Area 0, Process ID 100, Instance ID 0, Router ID 172.16.3.3
 Network Type MANET, Cost: 10 (dynamic), Cost Hysteresis: Disabled
 Cost Weights: Throughput 100, Resources 100, Latency 100, L2-factor 100
 Transmit Delay is 1 sec, State POINT_TO_MULTIPOINT,
 Timer intervals configured, Hello 5, Dead 20, Wait 20, Retransmit 5
   Hello due in 00:00:01
 Supports Link-local Signaling (LLS)
 Index 1/1/1, flood queue length 0
 Next 0x0(0)/0x0(0)/0x0(0)
 Last flood scan length is 2, maximum is 2
 Last flood scan time is 0 msec, maximum is 0 msec
 Neighbor Count is 1, Adjacent neighbor count is 1
 Adjacent with neighbor 2.2.2.2
 Suppress hello for 0 neighbor(s)
 Incremental Hello is enabled
 Local SCS number 1
```

```
 Relaying enabled
Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 12, maximum is 12
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 172.16.6.6  (Designated Router)
  Suppress hello for 0 neighbor(s)
Router#
```

Table 294 describes the significant fields shown in the display.

Table 294 show ospfv3 interface Field Descriptions

Field	Description
Ethernet0/0	Status of the physical link and the operational status of the protocol.
Link Local Address	Interface IPv6 address.
Area 0, Process ID 100, Instance ID 0, Router ID 172.16.3.3	Area ID, process ID, instance ID, and router ID of the area from which this route is learned.
Network Type MANET, Cost: 10 (dynamic), Cost hysteresis: Disabled	Network type and link-state cost.
Transmit Delay	Transmit delay, interface state, and router priority.
Timer intervals configured	Configuration of timer intervals, including hello-increment and dead-interval.
Hello due in 00:00:01	Number of seconds until the next hello packet is sent from this interface.
Supports Link-local Signaling (LLS)	Indicates that LLS is supported.
Last flood scan length is 2, maximum is 2	Indicates length of last flood scan and the maximum length.
Last flood scan time is 0 msec, maximum is 0 msec	Indicates how many milliseconds the last flood scan occurred and the maximum time length.
Neighbor Count	Count of network neighbors and a list of adjacent neighbors.
Adjacent with neighbor 2.2.2.2	Lists the adjacent neighbor.
Suppress hello for 0 neighbor(s)	Indicates the number of neighbors to suppress hello messages

show ospfv3 neighbor

To display Open Shortest Path First for IPv6 (OSPFv3) neighbor information on a per-interface basis, use the s**how ospfv3 neighbor** command in user EXEC or privileged EXEC mode.

show ospfv3 [*process-id*] [*area-id*] [*address-family*] **neighbor** [*interface-type interface-number*] [*neighbor-id*] [**detail**]

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
area-id	(Optional) Displays information only about a specified area.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
interface-type interface-number	(Optional) Interface type and number.
neighbor-id	(Optional) Neighbor ID.
detail	(Optional) Displays all neighbors in detail (lists all neighbors).

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Examples

The following is sample output from the **show ospfv3 neighbor** command:

```
Router# show ospfv3 neighbor

OSPFv3 Router with ID (42.1.1.1) (Process ID 42)
Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
44.4.4.4        1    FULL/  -        00:00:39    12              vm1

OSPFv3 Router with ID (1.1.1.1) (Process ID 100)
Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
4.4.4.4          1    FULL/  -        00:00:35    12              vm1
```

The following is sample output from the **show ospfv3 neighbor** command with the **detail** keyword for a Mobile Ad Hoc Network (MANET) environment:

```
Router# show ospfv3 neighbor detail
Neighbor 42.4.4.4, interface address 4.4.4.4
     In the process ID 42 area 0 via interface vmi1
Neighbor: interface-id 12, link-local address FE80::A8BB:CCFF:FE01:5800
     Neighbor priority is 1, State is FULL, 6 state changes
```

```
     Options is 0x000F12 in Hello (E-Bit, R-bit, AF-Bit, L-Bit, I-Bit, F-Bit)
     Options is 0x000112 in DBD (E-Bit, R-bit, AF-Bit)
     Dead timer due in 00:00:33
     Neighbor is up for 00:09:43
     Index 1/1/1, retransmission queue length 0, number of retransmission 0
     First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
     Last retransmission scan length is 0, maximum is 0
     Last retransmission scan time is 0 msec, maximum is 0 msec
     Neighbor is incremental Hello capable
     Last known SCS number 1
     Neighbor's willingness 128
     We are standby relay for the neighbor
     This neighbor is standby relay for us
     Neighbor is running Manet Version 10
Neighbor 4.4.4.4
      In the process ID 100 area 0 via interface vmi1
Neighbor: interface-id 12, link-local address FE80::A8BB:CCFF:FE01:5800
     Neighbor priority is 1, State is FULL, 6 state changes
     Options is 0x000E13 in Hello (V6-Bit, E-Bit, R-bit, L-Bit, I-Bit, F-Bit)
     Options is 0x000013 in DBD (V6-Bit, E-Bit, R-bit)
     Dead timer due in 00:00:37
     Neighbor is up for 00:09:43
     Index 1/1/1, retransmission queue length 0, number of retransmission 0
     First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
     Last retransmission scan length is 0, maximum is 0
     Last retransmission scan time is 0 msec, maximum is 0 msec
     Neighbor is incremental Hello capable
     Last known SCS number 1
     Neighbor's willingness 128
Two-hop neighbors:
     5.5.5.5
     We are standby relay for the neighbor
     This neighbor is active relay for us
     Neighbor is running Manet Version 10
     Selective Peering is enabled
     1 paths to this neighbor
Neighbor peering state: Slave, local peering state: Master,
     Default cost metric is 0
     Minimum incremental cost is 10
```

Table 295 describes the significant fields shown in the display.

Table 295 show ospfv3 neighbor Field Descriptions

Field	Description
Neighbor ID; Neighbor	Neighbor router ID.
In the area	Area and interface through which the OSPFv3 neighbor is known.
Pri; Neighbor priority	Router priority of the neighbor, neighbor state.
State	OSPFv3 state.
State changes	Number of state changes since the neighbor was created.
Options	Hello packet options field contents (E-bit only). Possible values are 0 and 2; 2 indicates area is not a stub; 0 indicates area is a stub.)
Dead timer due in	Expected time before Cisco IOS software declares the neighbor dead.

Table 295 show ospfv3 neighbor Field Descriptions (continued)

Field	Description
Neighbor is up for	Number of hours:minutes:seconds since the neighbor went into two-way state.
Index	Neighbor location in the area-wide and autonomous system-wide retransmission queue.
retransmission queue length	Number of elements in the retransmission queue.
number of retransmission	Number of times update packets have been resent during flooding.
First	Memory location of the flooding details.
Next	Memory location of the flooding details.
Last retransmission scan length	Number of link state advertisements (LSAs) in the last retransmission packet.
maximum	Maximum number of LSAs sent in any retransmission packet.
Last retransmission scan time	Time taken to build last retransmission packet.
maximum	Maximum time taken to build any retransmission packet.
Neighbor is incremental Hello capable	The MANET neighbor interface is capable of receiving increment hello messages. A neighbor must be capable of sending and receiving incremental hello packets to be a full neighbor on a MANET interface.
Last known SCS number 1	Indicates the last received MANET state. The State Change Sequence number is included in the incremental hello packet.
Neighbor's willingness 128	Indicates the neighbors willingness to act as an active relay for this router, on a scale of 0 (not willing) to 255 (always willing). Willingness is used as a tiebreaker when electing an active relay.
We are standby relay for neighbor	Indicates that this router will not flood LSAs received from this neighbor until one or more of its neighbors fails to acknowledge receiving the LSA flood from another neighbor.
Neighbor is running Manet Version 10	Indicates the MANET version number. Routers cannot establish full adjacency unless they are running the same MANET version.
Two-hop neighbors	Lists the router IDs of all full neighbors of the specified router that are not also neighbors of this router.
Selective Peering is enabled	The MANET interface has selective peering enabled.

Table 295 show ospfv3 neighbor Field Descriptions (continued)

Field	Description
1 paths to this neighbor	Indicates the number of unique paths to this router that exist in the routing table. This number might exceed the redundancy level configured for this OSPFv3 process.
Neighbor peering state...	Indicates which router is entitled to make the selective peering decision. Generally speaking, the entitled router has the smaller number of full neighbors at the time the routers discover each other.
Default cost metric is 0	Indicates the maximum OSPFv3 cost to a new neighbor to be considered for selective peering. If 0, a threshold OSPFv3 cost is not required for consideration.
Minimum incremental cost is 10	Indicates the minimum cost increment for the specified interface.

show ospfv3 request-list

To display a list of all link-state advertisements (LSAs) requested by a router, use the **show ospfv3 request-list** command in user EXEC or privileged EXEC mode.

show ospfv3 [*process-id*] [*area-id*] [*address-family*] **request-list** [*neighbor*] [*interface*] [*interface-neighbor*]

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the Open Shortest Path First version 3 (OSPFv3) routing process and can be a value from 1 through 65535.
area-id	(Optional) Displays information only about a specified area.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
neighbor	(Optional) Displays the list of all LSAs requested by the router from this neighbor.
interface	(Optional) Displays the list of all LSAs requested by the router from this interface.
interface-neighbor	(Optional) Displays the list of all LSAs requested by the router on this interface, from this neighbor.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

The information displayed by the **show ospfv3 request-list** command is useful in debugging OSPFv3 routing operations.

Examples

The following example shows information about the LSAs requested by the router:

```
Router# show ospfv3 request-list

            OSPFv3 Router with ID (192.168.255.5) (Process ID 1)

 Neighbor 192.168.255.2, interface Ethernet0/0 address
FE80::A8BB:CCFF:FE00:6600

 Type    LS ID           ADV RTR         Seq NO      Age    Checksum
  1      0.0.0.0         192.168.255.3   0x800000C2  1      0x0014C5
```

```
1       0.0.0.0         192.168.255.2   0x800000C8  0       0x000BCA
1       0.0.0.0         192.168.255.1   0x800000C5  1       0x008CD1
2       0.0.0.3         192.168.255.3   0x800000A9  774     0x0058C0
2       0.0.0.2         192.168.255.3   0x800000B7  1       0x003A63
```

Table 296 describes the significant fields shown in the display.

Table 296 show ospfv3 request-list Field Descriptions

Field	Description
OSPFv3 Router with ID (192.168.255.5) (Process ID 1)	Identification of the router for which information is displayed.
Interface Ethernet0/0	Interface for which information is displayed.
Type	Type of LSA.
LS ID	Link-state ID of the LSA.
ADV RTR	IP address of advertising router.
Seq NO	Sequence number of LSA.
Age	Age of LSA (in seconds).
Checksum	Checksum of LSA.

show ospfv3 retransmission-list

To display a list of all link-state advertisements (LSAs) waiting to be re-sent, use the **show ospfv3 retransmission-list** command in user EXEC or privileged EXEC mode.

show ospfv3 [*process-id*] [*area-id*] [*address-family*] **retransmission-list** [*neighbor*] [*interface*] [*interface-neighbor*]

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the Open Shortest Path First version 3 (OSPFv3) routing process and can be a value from 1 through 65535.
area-id	(Optional) Displays information only about a specified area.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
neighbor	(Optional) Displays the list of all LSAs waiting to be re-sent for this neighbor.
interface	(Optional) Displays the list of all LSAs waiting to be re-sent on this interface.
interface-neighbor	(Optional) Displays the list of all LSAs waiting to be re-sent on this interface, from this neighbor.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

The information displayed by the **show ospfv3 retransmission-list** command is useful in debugging Open Shortest Path First version 3 (OSPFv3) routing operations.

Examples

The following is sample output from the **show ospfv3 retransmission-list** command:

```
Router# show ospfv3 retransmission-list

        OSPFv3 Router with ID (192.168.255.2) (Process ID 1)

 Neighbor 192.168.255.1, interface Ethernet0/0
 Link state retransmission due in 3759 msec, Queue length 1

 Type    LS ID           ADV RTR         Seq NO      Age    Checksum
 0x2001  0               192.168.255.2   0x80000222  1      0x00AE52
```

Table 297 describes the significant fields shown in the display.

Table 297 show ospfv3 retransmission-list Field Descriptions

Field	Description
OSPFv3 Router with ID (192.168.255.2) (Process ID 1)	Identification of the router for which information is displayed.
Interface Ethernet0/0	Interface for which information is displayed.
Link state retransmission due in	Length of time before next link-state transmission.
Queue length	Number of elements in the retransmission queue.
Type	Type of LSA.
LS ID	Link-state ID of the LSA.
ADV RTR	IP address of advertising router.
Seq NO	Sequence number of the LSA.
Age	Age of LSA (in seconds).
Checksum	Checksum of LSA.

show ospfv3 statistic

To display Open Shortest Path First version 3 (OSPFv3) shortest path first (SPF) calculation statistics, use the **show ospfv3 statistic** command in user EXEC or privileged EXEC mode.

show ospfv3 [*process-id*] [*address-family*] **statistic** [**detail**]

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
detail	(Optional) Displays statistics separately for each OSPFv3 area and includes additional, more detailed statistics.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

The **show ospfv3 statistics** command provides important information about SPF calculations and the events that trigger them. This information can be meaningful for both OSPF network maintenance and troubleshooting. For example, entering the **show ospfv3 statistics** command is recommended as the first troubleshooting step for link-state advertisement (LSA) flapping.

Examples

The following example provides detailed statistics for each OSPFv3 area:

```
Router# show ospfv3 statistics detail

  Area 0: SPF algorithm executed 3 times

SPF 1 executed 00:06:57 ago, SPF type Full
  SPF calculation time (in msec):
  SPT    Prefix D-Int  Sum    D-Sum  Ext    D-Ext  Total
  0      0      0      0      0      0      0      0
  RIB manipulation time (in msec):
  RIB Update    RIB Delete
  0             0
  LSIDs processed R:1 N:0 Prefix:0 SN:0 SA:0 X7:0
  Change record R N SN SA L
  LSAs changed 1
  Changed LSAs. Recorded is Advertising Router, LSID and LS type:
  10.2.2.2/0(R)
```

```
SPF 2 executed 00:06:47 ago, SPF type Full
  SPF calculation time (in msec):
  SPT    Prefix D-Int  Sum    D-Sum  Ext    D-Ext  Total
  0      0      0      0      0      0      0      0
  RIB manipulation time (in msec):
  RIB Update    RIB Delete
  0             0
  LSIDs processed R:1 N:0 Prefix:1 SN:0 SA:0 X7:0
  Change record R L P
  LSAs changed 4
  Changed LSAs. Recorded is Advertising Router, LSID and LS type:
  10.2.2.2/2(L) 10.2.2.2/0(R) 10.2.2.2/2(L) 10.2.2.2/0(P)
```

Table 267 describes the significant fields shown in the display.

Table 298 show ospfv3 statistics Field Descriptions

Field	Description
Area	OSPF area ID.
SPF	Number of SPF algorithms executed in the OSPF area. The number increases by one for each SPF algorithm that is executed in the area.
Executed ago	Time in milliseconds that has passed between the start of the SPF algorithm execution and the current time.
SPF type	SPF type can be Full or Incremental.
SPT	Time in milliseconds required to compute the first stage of the SPF algorithm (to build a short path tree). The SPT time plus the time required to process links to stub networks equals the Intra time.
Ext	Time in milliseconds for the SPF algorithm to process external and not so stubby area (NSSA) LSAs and to install external and NSSA routes in the routing table.
Total	Total duration time in milliseconds for the SPF algorithm process.
LSIDs processed	Number of LSAs processed during the SPF calculation: • N—Network LSA. • R—Router LSA. • SA—Summary Autonomous System Boundary Router (ASBR) (SA) LSA. • SN—Summary Network (SN) LSA. • Stub—Stub links. • X7—External Type-7 (X7) LSA.

show ospfv3 summary-prefix

To display a list of all summary address redistribution information configured under an Open Shortest Path First version 3 (OSPFv3) process, use the **show ospfv3 summary-prefix** command in user EXEC or privileged EXEC mode.

show ospfv3 [*process-id*] [*address-family*] **summary-prefix**

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

The *process-id* argument can be entered as a decimal number or as an IPv6 address format.

Examples

The following is sample output from the **show ospfv3 summary-prefix** command:

```
Router# show ospfv3 summary-prefix

OSPFv3 Process 1, Summary-prefix

FEC0::/24 Metric 16777215, Type 0, Tag 0
```

Table 299 describes the significant fields shown in the display.

Table 299 show ospfv3 summary-prefix Field Descriptions

Field	Description
OSPFv3 Process	Process ID of the router for which information is displayed.
Metric	Metric used to reach the destination router.
Type	Type of link-state advertisement (LSA).
Tag	LSA tag.

show ospfv3 timers rate-limit

To display all of the link-state advertisements (LSAs) in the rate limit queue, use the **show ospfv3 timers rate-limit** command in privileged EXEC mode.

show ospfv3 [*process-id*] [*address-family*] **timers rate-limit**

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

Use the **show ospfv3 timers rate-limit** command to discover when LSAs in the queue will be sent.

Examples

The following is sample output from the **show ospfv3 timers rate-limit** command:

```
Router# show ospfv3 timers rate-limit

List of LSAs that are in rate limit Queue

    LSAID: 0.0.0.0 Type: 0x2001 Adv Rtr: 55.55.55.55 Due in: 00:00:00.500
    LSAID: 0.0.0.0 Type: 0x2009 Adv Rtr: 55.55.55.55 Due in: 00:00:00.500
```

Table 300 describes the significant fields shown in the display.

Table 300 show ospfv3 timers rate-limit Field Descriptions

Field	Description
LSAID	ID of the LSA.
Type	Type of LSA.
Adv Rtr	ID of the advertising router.
Due in:	When the LSA is scheduled to be sent (in hours:minutes:seconds).

show ospfv3 traffic

To display Open Shortest Path First version 3 (OSPFv3) traffic statistics, use the **show ospfv3 traffic** command in privileged EXEC mode.

show ospfv3 [*process-id*] [*address-family*] **traffic** [*interface-type interface-number*]

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
interface-type interface-number	(Optional) Type and number associated with a specific OSPFv3 interface.

Command Default

When the **show ospfv3 traffic** command is entered without any arguments, global OSPFv3 traffic statistics are displayed, including queue statistics for each OSPFv3 process, statistics for each interface, and per OSPFv3 process statistics.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

You can limit the displayed traffic statistics to those for a specific OSPFv3 process by entering a value for the *process-id* argument, or you can limit output to traffic statistics for a specific interface associated with an OSPFv3 process by entering values for the *interface-type* and *interface-number* arguments.

Examples

The following example shows the display output for the **show ospfv3 traffic** command for OSPFv3:

```
Router# show ospfv3 traffic

OSPFv3 statistics:
  Rcvd: 32 total, 0 checksum errors
        10 hello, 7 database desc, 2 link state req
        9 link state updates, 4 link state acks
        0 LSA ignored

  Sent: 45 total, 0 failed
        17 hello, 12 database desc, 2 link state req
        8 link state updates, 6 link state acks
```

```
        OSPFv3 Router with ID (10.1.1.4) (Process ID 6)

OSPFv3 queues statistic for process ID 6
  Hello queue size 0, no limit, max size 2
  Router queue size 0, limit 200, drops 0, max size 2


Interface statistics:


    Interface Serial2/0

OSPFv3 packets received/sent

  Type          Packets              Bytes
  RX Invalid    0                    0
  RX Hello      5                    196
  RX DB des     4                    172
  RX LS req     1                    52
  RX LS upd     4                    320
  RX LS ack     2                    112
  RX Total      16                   852

  TX Failed     0                    0
  TX Hello      8                    304
  TX DB des     3                    144
  TX LS req     1                    52
  TX LS upd     3                    252
  TX LS ack     3                    148
  TX Total      18                   900

OSPFv3 header errors
  Length 0, Checksum 0, Version 0, No Virtual Link 0,
  Area Mismatch 0, Self Originated 0, Duplicate ID 0,
  Instance ID 0, Hello 0, MTU Mismatch 0,
  Nbr Ignored 0, Authentication 0,

OSPFv3 LSA errors
  Type 0, Length 0, Data 0, Checksum 0,


    Interface Ethernet0/0

OSPFv3 packets received/sent

  Type          Packets              Bytes
  RX Invalid    0                    0
  RX Hello      6                    240
  RX DB des     3                    144
  RX LS req     1                    52
  RX LS upd     5                    372
  RX LS ack     2                    152
  RX Total      17                   960

  TX Failed     0                    0
  TX Hello      11                   420
  TX DB des     9                    312
  TX LS req     1                    52
  TX LS upd     5                    376
  TX LS ack     3                    148
  TX Total      29                   1308
```

```
OSPFv3 header errors
  Length 0, Checksum 0, Version 0, No Virtual Link 0,
  Area Mismatch 0, Self Originated 0, Duplicate ID 0,
  Instance ID 0, Hello 0, MTU Mismatch 0,
  Nbr Ignored 0, Authentication 0,

OSPFv3 LSA errors
  Type 0, Length 0, Data 0, Checksum 0,


Summary traffic statistics for process ID 6:

OSPFv3 packets received/sent

  Type          Packets              Bytes
  RX Invalid    0                    0
  RX Hello      11                   436
  RX DB des     7                    316
  RX LS req     2                    104
  RX LS upd     9                    692
  RX LS ack     4                    264
  RX Total      33                   1812

  TX Failed     0                    0
  TX Hello      19                   724
  TX DB des     12                   456
  TX LS req     2                    104
  TX LS upd     8                    628
  TX LS ack     6                    296
  TX Total      47                   2208

OSPFv3 header errors
  Length 0, Checksum 0, Version 0, No Virtual Link 0,
  Area Mismatch 0, Self Originated 0, Duplicate ID 0,
  Instance ID 0, Hello 0, MTU Mismatch 0,
  Nbr Ignored 0, Authentication 0,

OSPFv3 LSA errors
  Type 0, Length 0, Data 0, Checksum 0,
```

Table 301 describes the significant fields shown in the display.

Table 301 show ospfv3 traffic Field Descriptions

Field	Description
OSPFv3 statistics	Traffic statistics accumulated for all OSPFv3 processes running on the router. To ensure compatibility with the **show ip traffic** command, only checksum errors are displayed. Identifies the route map name.
OSPFv3 queues statistic for process ID	Queue statistics specific to Cisco IOS software.
Hello queue	Statistics for the internal Cisco IOS queue between the packet switching code (process IP Input) and the OSPFv3 hello process for all received OSPFv3 packets.
Router queue	Statistics for the internal Cisco IOS queue between the OSPFv3 hello process and the OSPFv3 router for all received OSPFv3 packets except OSPFv3 hellos.

Table 301 show ospfv3 traffic Field Descriptions (continued)

Field	Description
queue size	Actual size of the queue.
queue limit	Maximum allowed size of the queue.
queue max size	Maximum recorded size of the queue.
Interface statistics	Per-interface traffic statistics for all interfaces that belong to the specific OSPFv3 process ID.
OSPFv3 packets received/sent	Number of OSPFv3 packets received and sent on the interface, sorted by packet types.
OSPFv3 header errors	Packet appears in this section if it was discarded because of an error in the header of an OSPFv3 packet. The discarded packet is counted under the appropriate discard reason.
OSPFv3 LSA errors	Packet appears in this section if it was discarded because of an error in the header of an OSPFv3 link-state advertisement (LSA). The discarded packet is counted under the appropriate discard reason.
Summary traffic statistics for process ID	Summary traffic statistics accumulated for an OSPFv3 process. **Note** The OSPFv3 process ID is a unique value assigned to the OSPFv3 process in the configuration. The value for the received errors is the sum of the OSPFv3 header errors that are detected by the OSPFv3 process, unlike the sum of the checksum errors that are listed in the global OSPFv3 statistics.

show ospfv3 virtual-links

To display parameters and the current state of Open Shortest Path First version 3 (OSPFv3) virtual links, use the **show ospfv3 virtual-links** command in user EXEC or privileged EXEC mode.

show ospfv3 [*process-id*] [*address-family*] **virtual-links**

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

The information displayed by the **show ospfv3 virtual-links** command is useful in debugging OSPFv3 routing operations.

Examples

The following is sample output from the **show ospfv3 virtual-links** command:

```
Router# show ospfv3 virtual-links

Virtual Link OSPF_VL0 to router 172.16.6.6 is up
  Interface ID 27, IPv6 address FEC0:6666:6666::
  Run as demand circuit
  DoNotAge LSA allowed.
  Transit area 2, via interface ATM3/0, Cost of using 1
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
```

Table 302 describes the significant fields shown in the display.

Table 302 show ospfv3 virtual-links Field Descriptions

Field	Description
Virtual Link OSPF_VL0 to router 172.16.6.6 is up	Specifies the OSPFv3 neighbor, and if the link to that neighbor is up or down.
Interface ID	Interface ID and IPv6 address of the router.
Transit area 2	The transit area through which the virtual link is formed.
via interface ATM3/0	The interface through which the virtual link is formed.
Cost of using 1	The cost of reaching the OSPFv3 neighbor through the virtual link.
Transmit Delay is 1 sec	The transmit delay (in seconds) on the virtual link.
State POINT_TO_POINT	The state of the OSPFv3 neighbor.
Timer intervals...	The various timer intervals configured for the link.
Hello due in 0:00:06	When the next hello is expected from the neighbor.

The following sample output from the **show ospfv3 virtual-links** command has two virtual links. One is protected by authentication, and the other is protected by encryption.

```
Router# show ospfv3 virtual-links

Virtual Link OSPFv3_VL1 to router 10.2.0.1 is up
   Interface ID 69, IPv6 address 2001:0DB8:11:0:A8BB:CCFF:FE00:6A00
   Run as demand circuit
   DoNotAge LSA allowed.
   Transit area 1, via interface Serial12/0, Cost of using 64
   NULL encryption SHA-1 auth SPI 3944, secure socket UP (errors: 0)
   Transmit Delay is 1 sec, State POINT_TO_POINT,
   Timer intervals configured, Hello 2, Dead 10, Wait 40, Retransmit 5
     Adjacency State FULL (Hello suppressed)
     Index 1/2/4, retransmission queue length 0, number of retransmission 1
     First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
     Last retransmission scan length is 1, maximum is 1
     Last retransmission scan time is 0 msec, maximum is 0 msec
Virtual Link OSPFv3_VL0 to router 10.1.0.1 is up
   Interface ID 67, IPv6 address 2001:0DB8:13:0:A8BB:CCFF:FE00:6700
   Run as demand circuit
   DoNotAge LSA allowed.
   Transit area 1, via interface Serial11/0, Cost of using 128
   MD5 authentication SPI 940, secure socket UP (errors: 0)
   Transmit Delay is 1 sec, State POINT_TO_POINT,
   Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
     Adjacency State FULL (Hello suppressed)
     Index 1/1/3, retransmission queue length 0, number of retransmission 1
First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
     Last retransmission scan length is 1, maximum is 1
     Last retransmission scan time is 0 msec, maximum is 0 msec
```

show platform software ipv6-multicast

To display information about the platform software for IPv6 multicast, use the **show platform software ipv6-multicast** command in privileged EXEC mode.

show platform software ipv6-multicast {**acl-exception** | **acl-table** | **capability** | **connected** | **shared-adjacencies** | **statistics** | **summary**}

Syntax Description

acl-exception	Displays the IPv6-multicast entries that were switched in the software due to ACL exceptions.
acl-table	Displays the IPv6-multicast access list (ACL) request table entries.
capability	Displays the hardware capabilities.
connected	Displays the IPv6-multicast subnet/connected hardware entries.
shared-adjacencies	Displays the IPv6-multicast shared adjacencies.
statistics	Displays the internal software-based statistics.
summary	Displays the IPv6-multicast hardware-shortcut count.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXD	This command was introduced on the Supervisor Engine 720 and the Supervisor Engine 2.
12.2(18)SXE	This command was changed as follows: • Add the **acl-exception**, **acl-table**, and the **statistics** keywords on the Supervisor Engine 720 only. • Update the **show platform software ipv6-multicast capability** command output to include replication information.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to display the IPv6-hardware capabilities:

```
Router# show platform software ipv6-multicast capability

 Hardware switching for ipv6 is Enabled
 (S,G) forwarding for ipv6 supported using Netflow
 (*,G) bridging for ipv6 is supported using Fib
 Directly-connected entries for IPv6 is supported using ACL-TCAM.

Current System HW Replication Mode : Egress
Audo-detection of Replication Mode : ON

Slot Replication-Capability Replication-Mode
   2 Egress                 Egress
   5 Egress                 Egress
```

This example shows how to display the IPv6-multicast subnet/connected-hardware entries:

```
Router# show platform software ipv6-multicast connected

IPv6 Multicast Subnet entries
Flags : H - Installed in ACL-TCAM
        X - Not installed in ACL-TCAM due to
            label-full exception

Interface: Vlan40 [ H ]
         S:40::1 G:FF00::
         S:0:5000::2 G:FF00::
         S:5000::2 G:FF00::
Interface: Vlan30 [ H ]
         S:30::1 G:FF00::
Interface: Vlan20 [ H ]
         S:20::1 G:FF00::
Interface: Vlan10 [ H ]
         S:10::1 G:FF00::
```

This example shows how to display the IPv6-multicast shared adjacencies:

```
Router# show platform software ipv6-multicast shared-adjacencies

---- SLOT [7] ----

Shared IPv6 Mcast Adjacencies Index  Packets       Bytes
----------------------------- ------ ------------ ------------------
Subnet bridge adjacency       0x7F802  0            0
Control bridge adjacency      0x7      0            0
StarG_M bridge adjacency      0x8      0            0
S_G bridge adjacency          0x9      0            0
Default drop adjacency        0xA      0            0
StarG (spt == INF) adjacency  0xB      0            0
StarG (spt != INF) adjacency  0xC      0            0
```

This example shows how to display the IPv6-multicast statistics information:

```
Router# show platform software ipv6-multicast statistics

IPv6 Multicast HW-switching Status                : Enabled
IPv6 Multicast (*,G) HW-switching Status          : Disabled
IPv6 Multicast Subnet-entries Status              : Enabled
Default MFIB IPv6-table                           : 0x5108F770
(S,G,C) flowmask index                            : 3
(*,G,C) flowmask index                            : 65535

General Counters
-------------------------------------------------+------+
Mfib-hw-entries count                            0
Mfib-add count                                   4
Mfib-modify count                                2
Mfib-delete count                                2
Mfib-NP-entries count                            0
Mfib-D-entries count                             0
Mfib-IC-entries count                            0
Error Counters
-------------------------------------------------+------+
ACL flowmask err count                           0
ACL TCAM exptn count                             0
ACL renable count                                0
Idb Null error                                   0
```

This example shows how to display the IPv6-multicast hardware shortcut count:

```
Router# show platform software ipv6-multicast summary

IPv6 Multicast Netflow SC summary on Slot[7]:
Shortcut Type               Shortcut count
---------------------------+--------------
(S, G)                      0

IPv6 Multicast FIB SC summary on Slot[7]:
Shortcut Type               Shortcut count
---------------------------+--------------
(*, G/128)                  0
(*, G/m)                    0
```

Related Commands

Command	Description
ipv6 mfib hardware-switching	Configures hardware switching for IPv6 multicast packets on a global basis.

show platform software vpn

To display information about the platform software for IPv6 Virtual Private Networks (VPNs), use the **show platform software vpn** command in privileged EXEC mode.

show platform software vpn [**status** | **mapping ios**]

Syntax Description

status	(Optional) Displays the VPN status.
mapping ios	(Optional) Displays the Cisco IOS mapping information.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(33)SRB1	This command was introduced on the Cisco 7600 series routers.
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.

Usage Guidelines

If no keyword is used, then all VPN information is displayed.

Examples

The following example shows output regarding platform software for all VPNs:

```
Router# show platform software vpn
```

show route-map

To display static and dynamic route maps, use the **show route-map** command in privileged EXEC mode.

show route-map [*map-name* | **dynamic** [*dynamic-map-name* | **application** [*application-name*]] | **all**] [**detailed**]

Syntax Description

map-name	(Optional) Name of a specific route map.
dynamic	(Optional) Displays dynamic route map information.
dynamic-map-name	(Optional) Name of a specific dynamic route map.
application	(Optional) Displays dynamic route maps based on applications.
application-name	(Optional) Name of a specific application.
all	(Optional) Displays all static and dynamic route maps.
detailed	(Optional) Displays the details of the access control lists (ACLs) that have been used in the **match** clauses for dynamic route maps.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S, and support for continue clauses was integrated into the command output.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(27)SBA	The output was enhanced to display dynamically assigned route maps to VRF tables.
12.2(15)T	An additional counter collect policy routing statistic was integrated into Cisco IOS Release 12.2(15)T.
12.3(2)T	Support for continue clauses was integrated into Cisco IOS Release 12.3(2)T.
12.2(17b)SXA	This command was integrated into Cisco IOS Release 12.2(17b)SXA.
12.3(7)T	The **dynamic**, **application**, and **all** keywords were added.
12.0(28)S	The support for recursive **next-hop** clause was added.
12.3(14)T	The support for recursive **next-hop** clause was integrated into Cisco IOS Release 12.3(14)T. Support for the map display extension functionality was added. The **detailed** keyword was added.
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.
Cisco IOS XE Release 2.2	In Cisco IOS XE Release 2.2 this command was introduced on the Cisco ASR 1000 Series Routers.
15.0(1)M	This command was modified. The **detailed** keyword was removed.
12.2(33)SXI4	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SXI4.

Usage Guidelines

You can view static and dynamic route maps with the **show route-map** command. For Cisco IOS Release 12.3(14)T and later 12.4 and 12.4T releases, you can display the ACL-specific information that pertains to the route map in the same display without having to execute a **show route-map** command to display each ACL that is associated with the route map.

Redistribution

Use the **route-map** global configuration command, and the **match** and **set** route-map configuration commands, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the match criteria—the conditions under which redistribution is allowed for the current route-map command. The **set** commands specify the set actions—the particular redistribution actions to perform if the criteria enforced by the match commands are met. The **no route-map** command deletes the route map.

The **match route-map** configuration command has multiple formats. The **match** commands can be given in any order, and all match commands must "pass" to cause the route to be redistributed according to the set actions given with the set commands. The **no** forms of the **match** commands remove the specified match criteria.

Use **route maps** when you want detailed control over how routes are redistributed between routing processes. The destination routing protocol is the one you specify with the router global configuration command. The source routing protocol is the one you specify with the **redistribute** router configuration command. See the "Examples" section for an illustration of how route maps are configured.

When you are passing routes through a route map, a route map can have several parts. Any route that does not match at least one match clause relating to a **route-map** command will be ignored; that is, the route will not be advertised for outbound route maps and will not be accepted for inbound route maps. If you want to modify only some data, you must configure a second route map section with an explicit match specified.

Examples

The **show route-map** command will display configured route-maps, match, set, and continue clauses. The output will vary depending on which keywords are included with the command, and which software image is running in your router, as shown in the following examples:

- show route-map Command with No Keywords Specified: Example, page 2132
- show route-map Command with Dynamic Route Map Specified: Example, page 2134
- show route-map Command with Detailed ACL Information for Route Maps Specified: Example, page 2135
- show route-map Command with VRF Autoclassification: Example, page 2135

show route-map Command with No Keywords Specified: Example

The following is sample output from the **show route-map** command:

```
Router# show route-map

route-map ROUTE-MAP-NAME, permit, sequence 10
  Match clauses:
    ip address (access-lists): 1
    metric 10
  Continue: sequence 40
  Set clauses:
    as-path prepend 10
  Policy routing matches: 0 packets, 0 bytes
route-map ROUTE-MAP-NAME, permit, sequence 20
```

```
  Match clauses:
    ip address (access-lists): 2
    metric 20
  Set clauses:
    as-path prepend 10 10
  Policy routing matches: 0 packets, 0 bytes
route-map ROUTE-MAP-NAME, permit, sequence 30
  Match clauses:
  Continue: to next entry 40
  Set clauses:
    as-path prepend 10 10 10
  Policy routing matches: 0 packets, 0 bytes
route-map ROUTE-MAP-NAME, deny, sequence 40
  Match clauses:
    community (community-list filter): 20:2
  Set clauses:
    local-preference 100
  Policy routing matches: 0 packets, 0 bytes
route-map LOCAL-POLICY-MAP, permit, sequence 10
  Match clauses:
  Set clauses:
    community 655370
  Policy routing matches: 0 packets, 0 bytes
```

The following example shows Multiprotocol Label Switching (MPLS)-related route map information:

```
Router# show route-map

route-map OUT, permit, sequence 10
Match clauses:
  ip address (access-lists): 1
Set clauses:
  mpls label
Policy routing matches: 0 packets, 0 bytes

route-map IN, permit, sequence 10
Match clauses:
  ip address (access-lists): 2
  mpls label
Set clauses:
Policy routing matches: 0 packets, 0 bytes
```

Table 301 describes the significant fields shown in the display.

Table 303 show route-map Field Descriptions

Field	Description
route-map ROUTE-MAP-NAME	Name of the route map.
permit	Indicates that the route is redistributed as controlled by the set actions.
sequence	Number that indicates the position a new route map is to have in the list of route maps already configured with the same name.
Match clauses: tag	Match criteria—Conditions under which redistribution is allowed for the current route map.
Continue:	Continue clause—Shows the configuration of a continue clause and the route-map entry sequence number that the continue clause will go to.

Table 303 show route-map Field Descriptions (continued)

Field	Description
Set clauses: metric	Set actions—The particular redistribution actions to perform if the criteria enforced by the **match** commands are met.
Policy routing matches:	Number of packets and bytes that have been filtered by policy routing.

show route-map Command with Dynamic Route Map Specified: Example

The following is sample output from the **show route-map** command when entered with the **dynamic** keyword:

```
Router# show route-map dynamic

route-map AAA-02/06/04-14:01:26.619-1-AppSpec, permit, sequence 0, identifier 1137954548
  Match clauses:
    ip address (access-lists): PBR#1 PBR#2
  Set clauses:
  Policy routing matches: 0 packets, 0 bytes
route-map AAA-02/06/04-14:01:26.619-1-AppSpec, permit, sequence 1, identifier 1137956424
  Match clauses:
    ip address (access-lists): PBR#3 PBR#4
  Set clauses:
  Policy routing matches: 0 packets, 0 bytes
route-map AAA-02/06/04-14:01:26.619-1-AppSpec, permit, sequence 2, identifier 1124436704
  Match clauses:
    ip address (access-lists): PBR#5 PBR#6
    length 10 100
  Set clauses:
    ip next-hop 172.16.1.1
    ip gateway 172.16.1.1
  Policy routing matches: 0 packets, 0 bytes
Current active dynamic routemaps = 1
```

The following is sample output from the **show route-map** command when entered with the **dynamic** and **application** keywords:

```
Router# show route-map dynamic application

Application - AAA
  Number of active routemaps = 1
```

When you specify an application name, only dynamic routes for that application are shown. The following is sample output from the **show route-map** command when entered with the **dynamic** and **application** keywords and the AAA application name:

```
Router# show route-map dynamic application AAA

AAA
  Number of active rmaps = 2
AAA-02/06/04-14:01:26.619-1-AppSpec
AAA-02/06/04-14:34:09.735-2-AppSpec

Router# show route-map dynamic AAA-02/06/04-14:34:09.735-2-AppSpec

route-map AAA-02/06/04-14:34:09.735-2-AppSpec, permit, sequence 0, identifier 1128046100
  Match clauses:
    ip address (access-lists): PBR#7 PBR#8
  Set clauses:
  Policy routing matches: 0 packets, 0 bytes
```

```
route-map AAA-02/06/04-14:34:09.735-2-AppSpec, permit, sequence 1, identifier 1141277624
  Match clauses:
    ip address (access-lists): PBR#9 PBR#10
  Set clauses:
  Policy routing matches: 0 packets, 0 bytes
route-map AAA-02/06/04-14:34:09.735-2-AppSpec, permit, sequence 2, identifier 1141279420
  Match clauses:
    ip address (access-lists): PBR#11 PBR#12
    length 10 100
  Set clauses:
    ip next-hop 172.16.1.12
    ip gateway 172.16.1.12
  Policy routing matches: 0 packets, 0 bytes
Current active dynamic routemaps = 2
```

show route-map Command with Detailed ACL Information for Route Maps Specified: Example

The following is sample output from the **show route-map** command with the **dynamic** and **detailed** keywords entered:

```
Router# show route-map dynamic detailed

route-map AAA-01/20/04-22:03:10.799-1-AppSpec, permit, sequence 1, identifier 29675368
Match clauses:
ip address (access-lists):
Extended IP access list PBR#3
1 permit icmp 0.0.16.12 1.204.167.240 10.1.1.0 0.0.0.255 syn dscp af12 log-input fragments
Extended IP access list PBR#4
1 permit icmp 0.0.16.12 1.204.167.240 10.1.1.0 0.0.0.255 syn dscp af12 log-input fragments
Set clauses:
ip next-hop 172.16.1.14
ip gateway 172.16.1.14
Policy routing matches: 0 packets, 0 bytes
```

show route-map Command with VRF Autoclassification: Example

The following is sample output from the **show route-map** command when a specified VRF is configured for VRF autoclassification:

```
Router# show route-map dynamic

route-map None-06/01/04-21:14:21.407-1-IP VRF, permit, sequence 0
identifier 1675771000
 Match clauses:
 Set clauses: vrf red
 Policy routing matches: 0 packets, 0 bytes
Current active dynamic routemaps = 1
```

Related Commands

Command	Description
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
match interface (IP)	Distributes any routes that have their next hop out one of the interfaces specified.
match ip next-hop	Redistributes any routes that have a next hop router address passed by one of the access lists specified.
match tag	Redistributes routes in the routing table that match the specified tags.

show sccp

To display Skinny Client Control Protocol (SCCP) information such as administrative and operational status, use the **show sccp** command in user EXEC or privileged EXEC mode.

show sccp [**all** | **ccm group** [*number*] | **connections** [**details** | **internal** | **rsvp** | **summary**] | **server** | **statistics** | **call-identifications** | **call-references**]

Syntax Description

all	(Optional) Specifies all Skinny Client Control Protocol (SCCP) global information.
ccm	(Optional) Displays SCCP Cisco Unified Communications Manager (CUCM) group related information.
group	(Optional) Displays CUCM groups.
number	(Optional) CUCM group number that needs to be displayed.
connections	(Optional) Specifies information about the connections controlled by the SCCP transcoding and conferencing applications.
details	(Optional) Displays SCCP connections in detail.
internal	(Optional) Displays information about SCCP internal connections.
rsvp	(Optional) Displays Resource Reservation Protocol (RSVP) information about SCCP connections.
summary	(Optional) Displays information about SCCP connections.
server	(Optional) Displays SCCP server information.
statistics	(Optional) Specifies statistical information for SCCP transcoding and conferencing applications.
call-identifications	(Optional) Displays the following identification numbers that is associated with each leg of a call: • Session • Call Reference • Connection • Call • Bridge • Profile
call-references	(Optional) Displays codec, port, ID numbers for each leg of a call.

Command Modes

User EXEC
Privileged EXEC (#)

Command History

Release	Modification
12.1(5)YH	This command was introduced on the Cisco VG200.
12.2(6)T	This command was modified. The **rsvp** keyword was added.

Release	Modification
12.2(13)T	This command was implemented on the Cisco 2600 series, Cisco 3620, Cisco 3640, Cisco 3660, and Cisco 3700 series.
12.3(8)T	This command was modified. The following keywords and arguments were added: **ccm**, **connections**, **details**, **group**, **internal,** *number,* **summary**.
12.4(11)XW1	This command was modified. The stype field was added to the show output to show whether a connections is encrypted.
12.4(15)XY	This command was modified. The **statistics** and **server** keywords were added.
12.4(22)T	This command was modified. Command output was updated to show IPv6 information and it was integrated into Cisco IOS Release 12.2(13)T.
15.1(4)M	This command was modified. The **call-identifications** and **call-references** keywords were added.

Usage Guidelines

The router on which you use the **show sccp** command must be equipped with one or more digital T1/E1 packet voice trunk network modules (NM-HDVs) or high-density voice (HDV) transcoding/conferencing DSP farms (NM-HDV-FARMs) to provide digital signal processor (DSP) resources.

Use the **show sccp ccm** group command to show detailed information about all groups assigned to the Cisco Unified CallManager. The optional group-number argument can be added to select details about a specific group.

Configure the **show sccp server statistics** command on the Cisco Unified Border Element, IP-to-IP Gateway, or Session Border Controller where no SCCP phone is registered, to show the statistical counts on the SCCP server. The counts display queuing errors and message drops on the transcoder alone when it is on the Cisco Unified Border Element, IP-to-IP Gateway, or Session Border Controller.

When the **show sccp server statistics** command is used on the Cisco Unified Manager Express (CME), it is recommended for use together with the clear sccp server statistics command.

Examples

In the following sample output, the gateway IP address can be an IPv4 or IPv6 address when it operates on an IPv4/IPv6 dual stack.

```
Router# show sccp
SCCP Admin State: UP
Gateway Local Interface: GigabitEthernet0/0
        IPv6 Address: 2001:DB8:C18:1::3
        IPv4 Address: 10.4.34.100
        Port Number: 2000
IP Precedence: 5
User Masked Codec list: None
Call Manager: 172.19.242.27, Port Number: 2000
                Priority: N/A, Version: 5.0.1, Identifier: 4
                Trustpoint: N/A
Call Manager: 2001:DB8:C18:1::100, Port Number: 2000
                Priority: N/A, Version: 7.0, Identifier: 1
                Trustpoint: N/A
```

Table 304 describes the significant fields shown in the display.

Table 304 show sccp Field Descriptions

Field	Description
SCCP Admin State	Current state of the SCCP session.
Gateway Local Interface	Local interface that SCCP applications use to register with Cisco Unified Communications Manager.
IP precedence	Sets the IP precedence value for SCCP.
User Masked Codec list	Codec to mask.
Call Manager	Cisco Unified CallManager server information.

The following is sample output from this command for IPv4 only. The field descriptions are self-explanatory.

```
Router# show sccp

SCCP Admin State: UP
Gateway IP Address: 10.10.10.11, Port Number: 0
Switchover Method: IMMEDIATE, Switchback Method: GUARD_TIMER
Switchback Guard Timer: 1200 sec, IP Precedence: 5
Max Supported MTP sessions: 100
Transcoding Oper State: ACTIVE - Cause Code: NONE
Active CallManager: 10.10.10.35, Port Number: 2000
TCP Link Status: CONNECTED
Conferencing Oper State: DOWN - Cause Code: DSPFARM_DOWN
Active CallManager: NONE
TCP Link Status: NOT_CONNECTED
CallManager: 10.10.10.37, Port Number: 2000
Priority: 3, Version: 3.1
CallManager: 10.10.10.35, Port Number: 2000
Priority: 2, Version: 3.0
```

The following sample shows statistical information for SCCP transcoding and conferencing applications.

```
Router# show sccp statistics

SCCP Transcoding Application Statistics:
TCP packets rx 548, tx 559
Unsupported pkts rx 3, Unrecognized pkts rx 0
Register tx 3, successful 3, rejected 0, failed 0
KeepAlive tx 543, successful 540, failed 2
OpenReceiveChannel rx 2, successful 2, failed 0
CloseReceiveChannel rx 0, successful 0, failed 0
StartMediaTransmission rx 2, successful 2, failed 0
StopMediaTransmission rx 0, successful 0, failed 0
MediaStreamingFailure rx 0
Switchover 1, Switchback 1

SCCP Conferencing Application Statistics:
TCP packets rx 0, tx 0
Unsupported pkts rx 0, Unrecognized pkts rx 0
Register tx 0, successful 0, rejected 0, failed 0
KeepAlive tx 0, successful 0, failed 0
OpenReceiveChannel rx 0, successful 0, failed 0
CloseReceiveChannel rx 0, successful 0, failed 0
StartMediaTransmission rx 0, successful 0, failed 0
StopMediaTransmission rx 0, successful 0, failed 0
```

```
MediaStreamingFailure rx 0
Switchover 0, Switchback 0
```

In the following example, the secure value of the stype field indicates that the conection is encrypted. The field descriptions are self-explanatory.

```
Router# show sccp connections

sess_id    conn_id    stype        mode codec   ripaddr       rport sport

16777222   16777409   secure-xcode sendrecv g729b   10.3.56.120   16772 19534
16777222   16777393   secure-xcode sendrecv g711u   10.3.56.50    17030 18464

Total number of active session(s) 1, and connection(s) 2
```

The following example shows the remote IP addresses of active RTP sessions, each of which shows either an IPv4 or an IPv6 address.

```
Router# show sccp connections

sess_id  conn_id  stype  mode    codec sport rport ripaddr

16777219 16777245 conf  sendrecv g711u 16516 27814 10.3.43.46
16777219 16777242 conf  sendrecv g711u 17712 18028 10.3.43.2
16777219 16777232 conf  sendrecv g711u 16890 19440 10.3.43.2
16777219 16777228 conf  sendrecv g711u 19452 17464 10.3.43.2
16777220 16777229 xcode sendrecv g711u 17464 19452 10.3.43.2
16777220 16777227 xcode sendrecv g729b 19466 19434 2001:0DB8:C18:1:212:79FF:FED7:B254
16777221 16777233 mtp   sendrecv g711u 19440 16890 10.3.43.2
16777221 16777231 mtp   sendrecv g711u 17698 17426 2001:0DB8:C18:1:212:79FF:FED7:B254
16777223 16777243 mtp   sendrecv g711u 18028 17712 10.3.43.2
16777223 16777241 mtp   sendrecv g711u 16588 19446 2001:0DB8:C18:1:212:79FF:FED7:B254
```

The following is sample output for the two Cisco CallManager Groups assigned to the Cisco Unified CallManager: group 5 named "boston office" and group 988 named "atlanta office".

```
Router# show sccp ccm group

CCM Group Identifier: 5
 Description: boston office
 Binded Interface: NONE, IP Address: NONE
 Registration Retries: 3, Registration Timeout: 10 sec
 Keepalive Retries: 3, Keepalive Timeout: 30 sec
 CCM Connect Retries: 3, CCM Connect Interval: 1200 sec
 Switchover Method: GRACEFUL, Switchback Method: GRACEFUL_GUARD
 Switchback Interval: 10 sec, Switchback Timeout: 7200 sec
 Signaling DSCP value: default, Audio DSCP value: default

CCM Group Identifier: 988
 Description: atlanta office
 Binded Interface: NONE, IP Address: NONE
 Associated CCM Id: 1, Priority in this CCM Group: 1
 Associated Profile: 6, Registration Name: MTP123456789988
 Associated Profile: 10, Registration Name: CFB123456789966
 Registration Retries: 3, Registration Timeout: 10 sec
 Keepalive Retries: 5, Keepalive Timeout: 30 sec
 CCM Connect Retries: 3, CCM Connect Interval: 10 sec
 Switchover Method: IMMEDIATE, Switchback Method: IMMEDIATE
 Switchback Interval: 15 sec, Switchback Timeout: 0 sec
 Signaling DSCP value: default, Audio DSCP value: default
```

Table 305 describes the significant fields shown in the display.

Table 305 show sccp ccm group Field Descriptions

Field	Description
CCM Group Identifier	Current state of the SCCP session.
Description	Local interface that SCCP applications use to register with Cisco Unified Communications Manager.
Binded Interface	Sets the IP precedence value for SCCP.
Registration Retries	Codec to mask.
Registration Timeout	Cisco Unified CallManager server information.
Keepalive Retries	Displays the number of keepalive retries from Skinny Client Control Protocol (SCCP) to Cisco Unified CallManager.
Keepalive Timeout	Displays the number of times that a DSP farm attempts to connect to a Cisco Unified CallManager.
CCM Connect Retries	Displays the amount of time, in seconds, that a given DSP farm profile waits before attempting to connect to a Cisco Unified CallManager when the current Cisco Unified CallManager fails to connect.
CCM Connect Interval	Method that the SCCP client uses when the communication link between the active Cisco Unified CallManager and the SCCP client fails.
Switchover Method	Method used when the secondary Cisco Unified CallManager initiates the switchback process with that higher order Cisco Unified CallManager.
Switchback Method	Method used when the secondary Cisco Unified CallManager initiates the switchback process with that higher order Cisco Unified CallManager.
Switchback Interval	Amount of time that the DSP farm waits before polling the primary Cisco Unified CallManager when the current Cisco Unified CallManager switchback connection fails.
Switchback Timeout	Amount of time, in seconds, that the secondary Cisco Unified CallManager waits before switching back to the primary Cisco Unified CallManager.
Associated CCM Id	Number assigned to the Cisco Unified CallManager.
Registration Name	User-specified device name in Cisco Unified CallManager.
Associated Profile	Number of the DSP farm profile associated with the Cisco Unified CallManager group.

The following sample output displays the summary information for all SCCP call references:

```
Router# show sccp call-reference
session_id: 16805277   session_type: vcf  , profile_id: 101,
    call-reference: 25666614  , Name: , Number: 3004
        Audio conn_id: 16777929  , str_passthr: 0
              rtp-call-id: 21        , bridge-id: 15        , msp-call-id: 12
              mode: sendrecv, sport: 25146, rport 16648, ripaddr: 10.22.82.205
              codec: g711u  , pkt-period: 20
    call-reference: 25666611  , Name: , Number: 6628
        Audio conn_id: 16777926  , str_passthr: 0
              rtp-call-id: 19        , bridge-id: 13        , msp-call-id: 12
              mode: sendrecv, sport: 28168, rport 2398 , ripaddr: 128.107.147.125
              codec: g711u  , pkt-period: 20
        Video conn_id: 16777927  , conn_id_tx: 16777928  , str_passthr: 0
```

```
              rtp-call-id: 20        , bridge-id: 14        , msp-call-id: 12
              mode: sendrecv, sport: 22604, rport 2400 , ripaddr: 128.107.147.125
              bit rate: 1100kbps, frame rate: 30fps , rtp pt_rx: 97, rtp pt_tx: 97
              codec: h264, Profile: 0x40, level: 2.2, max mbps: 81 (x500 MB/s), max fs: 7
(x256 MBs)
    call-reference: 25666608  , Name: , Number: 62783365
        Audio conn_id: 16777923  , str_passthr: 0
              rtp-call-id: 16        , bridge-id: 11        , msp-call-id: 12
              mode: sendrecv, sport: 21490, rport 20590, ripaddr: 10.22.83.142
              codec: g711u  , pkt-period: 20
        Video conn_id: 16777924  , conn_id_tx: 16777925  , str_passthr: 0
              rtp-call-id: 17        , bridge-id: 12        , msp-call-id: 12
              mode: sendrecv, sport: 23868, rport 29010, ripaddr: 10.22.83.142
              bit rate: 960kbps, frame rate: 30fps , rtp pt_rx: 97, rtp pt_tx: 97
              codec: h264, Profile: 0x40, level: 3.0, max mbps: 0 (x500 MB/s), max fs: 0
(x256 MBs)
    call-reference: 25666602  , Name: , Number: 62783363
        Audio conn_id: 16777916  , str_passthr: 0
              rtp-call-id: 11        , bridge-id: 7         , msp-call-id: 12
              mode: sendrecv, sport: 26940, rport 20672, ripaddr: 10.22.82.48
              codec: g711u  , pkt-period: 20
        Video conn_id: 16777917  , conn_id_tx: 16777919  , str_passthr: 0
              rtp-call-id: 13        , bridge-id: 8         , msp-call-id: 12
              mode: sendrecv, sport: 16462, rport 20680, ripaddr: 10.22.82.48
              bit rate: 960kbps, frame rate: 30fps , rtp pt_rx: 97, rtp pt_tx: 97
              codec: h264, Profile: 0x40, level: 2.0, max mbps: 72 (x500 MB/s), max fs: 5
(x256 MBs)

Total number of active session(s) 1
   Total of number of active session(s) 1
      with total of number of call-reference(s) 4
         with total of number of audio connection(s) 4
         with total of number of video connection(s) 3
```

The following sample output displays summary information for all SCCP call identifications:

```
Router# show sccp call-identifications

sess_id   callref   conn_id   conn_id_tx spid  rtp_callid msp_callid bridge_id  codec
stype prof_id
16805277  25666614  16777929  0          0     21         12         15         g711u  vcf
101
16805277  25666611  16777926  0          0     19         12         13         g711u  vcf
101
16805277  25666611  16777927  16777928   0     20         12         14         h264   vcf
101
16805277  25666608  16777923  0          0     16         12         11         g711u  vcf
101
16805277  25666608  16777924  16777925   0     17         12         12         h264   vcf
101
16805277  25666602  16777916  0          0     11         12         7          g711u  vcf
101
16805277  25666602  16777917  16777919   0     13         12         8          h264   vcf
101

Total number of active session(s) 1
```

The following sample displays the output from **show sccp**:

```
Router# show sccp

SCCP Admin State: UP
Gateway Local Interface: GigabitEthernet0/1
        IPv4 Address: 172.19.156.7
        Port Number: 2000
```

```
IP Precedence: 5
User Masked Codec list: None
Call Manager: 1.4.211.39, Port Number: 2000
                Priority: N/A, Version: 7.0, Identifier: 1
                Trustpoint: N/A
Call Manager: 128.107.151.39, Port Number: 2000
                Priority: N/A, Version: 7.0, Identifier: 100
                Trustpoint: N/A

V_Conferencing Oper State: ACTIVE - Cause Code: NONE
Active Call Manager: 128.107.151.39, Port Number: 2000
TCP Link Status: CONNECTED, Profile Identifier: 101
Reported Max Streams: 4, Reported Max OOS Streams: 0
Layout: default 1x1
Supported Codec: g711ulaw, Maximum Packetization Period: 30
Supported Codec: g711alaw, Maximum Packetization Period: 30
Supported Codec: g729ar8, Maximum Packetization Period: 60
Supported Codec: g729abr8, Maximum Packetization Period: 60
Supported Codec: g729r8, Maximum Packetization Period: 60
Supported Codec: g729br8, Maximum Packetization Period: 60
Supported Codec: rfc2833 dtmf, Maximum Packetization Period: 30
Supported Codec: rfc2833 pass-thru, Maximum Packetization Period: 30
Supported Codec: inband-dtmf to rfc2833 conversion, Maximum Packetization Period: 30
Supported Codec: h264: QCIF, Frame Rate: 15fps, Bit Rate: 64-704 Kbps
Supported Codec: h264: QCIF, Frame Rate: 30fps, Bit Rate: 64-704 Kbps
Supported Codec: h264: CIF, Frame Rate: 15fps, Bit Rate: 64-704 Kbps
Supported Codec: h264: CIF, Frame Rate: 30fps, Bit Rate: 64-704 Kbps
Supported Codec: h264: 4CIF, Frame Rate: 30fps, Bit Rate: 1000-1000 Kbps
TLS : ENABLED
```

Related Commands

Command	Description
dsp service dspfarm	Configures DSP farm services for a specified voice card.
dspfarm (DSP farm)	Enables DSP-farm service.
dspfarm profile	Enters DSP farm profile configuration mode and defines a profile for DSP farm services.
sccp	Enables SCCP and its associated transcoding and conferencing applications.
show dspfarm	Displays summary information about DSP resources.

show sip-ua calls

To display active user agent client (UAC) and user agent server (UAS) information on Session Initiation Protocol (SIP) calls, use the **show sip-ua calls** command in privileged EXEC mode.

show sip-ua calls

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(22)T	Command output was updated to show IPv6 information and to display Resource Reservation Protocol (RSVP) quality of service (QoS) preconditions information.

Usage Guidelines

The **show sip-ua calls** command displays active UAC and UAS information for SIP calls on a Cisco IOS device. The output includes information about IPv6, RSVP, and media forking for each call on the device and for all media streams associated with the calls. There can be any number of media streams associated with a call, of which typically only one is active. However, a call can include up to three active media streams if the call is media-forked. Use this command when debugging multiple media streams to determine if an active call on the device is forked.

Examples

The following is sample output from the **show sip-ua calls** command for a forked call with four associated media streams, three of which are currently active:

```
Router# show sip-ua calls

SIP UAC CALL INFO

Call 1
SIP Call ID : 515205D4-20B711D6-8015FF77-1973C402@172.18.195.49
 State of the call : STATE_ACTIVE (6)
 Substate of the call : SUBSTATE_NONE (0)
 Calling Number : 5550200
 Called Number : 5551101
 Bit Flags : 0x12120030 0x220000
 Source IP Address (Sig ): 172.18.195.49
 Destn SIP Req Addr:Port : 172.18.207.18:5063
 Destn SIP Resp Addr:Port: 172.18.207.18:5063
 Destination Name : 172.18.207.18
 Number of Media Streams : 4
 Number of Active Streams: 3
 RTP Fork Object : 0x637C7B60
 Media Stream 1
  State of the stream : STREAM_ACTIVE
  Stream Call ID : 28
  Stream Type : voice-only (0)
  Negotiated Codec : g711ulaw (160 bytes)
  Codec Payload Type : 0
  Negotiated Dtmf-relay : inband-voice
```

```
  Dtmf-relay Payload Type : 0
  Media Source IP Addr:Port: 172.18.195.49:19444
  Media Dest IP Addr:Port : 172.18.193.190:16890
 Media Stream 2
  State of the stream : STREAM_ACTIVE
  Stream Call ID : 33
  Stream Type : voice+dtmf (1)
  Negotiated Codec : g711ulaw (160 bytes)
  Codec Payload Type : 0
  Negotiated Dtmf-relay : rtp-nte
  Dtmf-relay Payload Type : 101
  Media Source IP Addr:Port: 172.18.195.49:18928
  Media Dest IP Addr:Port : 172.18.195.73:18246
 Media Stream 3
  State of the stream : STREAM_ACTIVE
  Stream Call ID : 34
  Stream Type : dtmf-only (2)
  Negotiated Codec : No Codec (0 bytes)
  Codec Payload Type : -1 (None)
  Negotiated Dtmf-relay : rtp-nte
  Dtmf-relay Payload Type : 101
  Media Source IP Addr:Port: 172.18.195.49:18428
  Media Dest IP Addr:Port : 172.16.123.99:34463
 Media Stream 4
  State of the stream : STREAM_DEAD
  Stream Call ID : -1
  Stream Type : dtmf-only (2)
  Negotiated Codec : No Codec (0 bytes)
  Codec Payload Type : -1 (None)
  Negotiated Dtmf-relay : rtp-nte
  Dtmf-relay Payload Type : 101
  Media Source IP Addr:Port: 172.18.195.49:0
  Media Dest IP Addr:Port : 172.16.123.99:0

 Number of UAC calls: 1

SIP UAS CALL INFO

 Number of UAS calls: 0
```

The following is sample output from the **show sip-ua calls** command showing IPv6 information:

```
Router# show sip-ua calls

SIP UAC CALL INFO

Call 1
SIP Call ID                : 8368ED08-1C2A11DD-80078908-BA2972D0@2001::21B:D4FF:FED7:B000
   State of the call       : STATE_ACTIVE (7)
   Substate of the call    : SUBSTATE_NONE (0)
   Calling Number          : 2000
   Called Number           : 1000
   Bit Flags               : 0xC04018 0x100 0x0
   CC Call ID              : 2
   Source IP Address (Sig ): 2001::21B:D4FF:FED7:B000
   Destn SIP Req Addr:Port : [2001::21B:D5FF:FE1D:6C00]:5060
   Destn SIP Resp Addr:Port: [2001::21B:D5FF:FE1D:6C00]:5060
   Destination Name        : 2001::21B:D5FF:FE1D:6C00
   Number of Media Streams : 1
   Number of Active Streams: 1
   RTP Fork Object         : 0x0
   Media Mode              : flow-through
   Media Stream 1
     State of the stream      : STREAM_ACTIVE
```

```
     Stream Call ID           : 2
     Stream Type              : voice-only (0)
     Stream Media Addr Type   : 1709707780
     Negotiated Codec         :  (20 bytes)
     Codec Payload Type       : 18
     Negotiated Dtmf-relay    : inband-voice
     Dtmf-relay Payload Type  : 0
     Media Source IP Addr:Port: [2001::21B:D4FF:FED7:B000]:16504
     Media Dest IP Addr:Port  : [2001::21B:D5FF:FE1D:6C00]:19548

Options-Ping    ENABLED:NO    ACTIVE:NO
   Number of SIP User Agent Client(UAC) calls: 1

SIP UAS CALL INFO

   Number of SIP User Agent Server(UAS) calls: 0
```

The following is sample output from the **show sip-ua calls** command when mandatory QoS is configured at both endpoints and RSVP has succeeded:

```
Router# show sip-ua calls

SIP UAC CALL INFO

  Number of SIP User Agent Client(UAC) calls: 0

SIP UAS CALL INFO

Call 1
SIP Call ID              : F31FEA20-CFF411DC-8068DDB4-22C622B8@172.18.19.73
 State of the call       : STATE_ACTIVE (7)
 Substate of the call    : SUBSTATE_NONE (0)
 Calling Number          : 6001
 Called Number           : 1001
 Bit Flags               : 0x8C4401E 0x100 0x4
 CC Call ID              : 30
 Source IP Address (Sig ): 172.18.19.72
 Destn SIP Req Addr:Port : 172.18.19.73:5060
 Destn SIP Resp Addr:Port: 172.18.19.73:64440
 Destination Name        : 172.18.19.73
 Number of Media Streams : 1
 Number of Active Streams: 1
 RTP Fork Object         : 0x0
 Media Mode              : flow-through
 Media Stream 1
  State of the stream      : STREAM_ACTIVE
  Stream Call ID           : 30
  Stream Type              : voice-only (0)
  Negotiated Codec         : g711ulaw (160 bytes)
  Codec Payload Type       : 0
  Negotiated Dtmf-relay    : inband-voice
  Dtmf-relay Payload Type  : 0
  Media Source IP Addr:Port: 172.18.19.72:18542
  Media Dest IP Addr:Port  : 172.18.19.73:16912
  Orig Media Dest IP Addr:Port : 0.0.0.0:0
  QoS ID                   : -2
  Local QoS Strength       : Mandatory
  Negotiated QoS Strength  : Mandatory
  Negotiated QoS Direction : SendRecv
  Local QoS Status         : Success


Options-Ping    ENABLED:NO     ACTIVE:NO
 Number of SIP User Agent Server(UAS) calls: 1
```

The following is sample output from the **show sip-ua calls** command when optional QoS is configured at both endpoints and RSVP has succeeded:

```
Router# show sip-ua calls

SIP UAC CALL INFO

   Number of SIP User Agent Client(UAC) calls: 0

SIP UAS CALL INFO

Call 1
SIP Call ID              : 867EA226-D01311DC-8041CA97-F9A5F4F1@172.18.19.73
 State of the call       : STATE_ACTIVE (7)
 Substate of the call    : SUBSTATE_NONE (0)
 Calling Number          : 6001
 Called Number           : 1001
 Bit Flags               : 0x8C4401E 0x100 0x4
 CC Call ID              : 30
 Source IP Address (Sig ): 172.18.19.72
 Destn SIP Req Addr:Port : 172.18.19.73:5060
 Destn SIP Resp Addr:Port: 172.18.19.73:25055
 Destination Name        : 172.18.19.73
 Number of Media Streams : 1
 Number of Active Streams: 1
 RTP Fork Object         : 0x0
 Media Mode              : flow-through
 Media Stream 1
  State of the stream      : STREAM_ACTIVE
  Stream Call ID           : 30
  Stream Type              : voice-only (0)
  Negotiated Codec         : g711ulaw (160 bytes)
  Codec Payload Type       : 0
  Negotiated Dtmf-relay    : inband-voice
  Dtmf-relay Payload Type  : 0
  Media Source IP Addr:Port: 172.18.19.72:17556
  Media Dest IP Addr:Port  : 172.18.19.73:17966
  Orig Media Dest IP Addr:Port : 0.0.0.0:0
  QoS ID                   : -2
  Local QoS Strength       : Optional
  Negotiated QoS Strength  : Optional
  Negotiated QoS Direction : SendRecv
  Local QoS Status         : Success

Options-Ping    ENABLED:NO    ACTIVE:NO
   Number of SIP User Agent Server(UAS) calls: 1
```

The following is sample output from the **show sip-ua calls** command when optional QoS is configured at both endpoints and RSVP has failed:

```
Router# show sip-ua calls

SIP UAC CALL INFO

   Number of SIP User Agent Client(UAC) calls: 0

SIP UAS CALL INFO

Call 1
SIP Call ID              : 867EA226-D01311DC-8041CA97-F9A5F4F1@172.18.19.73
 State of the call       : STATE_ACTIVE (7)
 Substate of the call    : SUBSTATE_NONE (0)
```

```
 Calling Number          : 6001
 Called Number           : 1001
 Bit Flags               : 0x8C4401E 0x100 0x4
 CC Call ID              : 30
 Source IP Address (Sig ): 172.18.19.72
 Destn SIP Req Addr:Port : 172.18.19.73:5060
 Destn SIP Resp Addr:Port: 172.18.19.73:25055
 Destination Name        : 172.18.19.73
 Number of Media Streams : 1
 Number of Active Streams: 1
 RTP Fork Object         : 0x0
 Media Mode              : flow-through
 Media Stream 1
  State of the stream      : STREAM_ACTIVE
  Stream Call ID           : 30
  Stream Type              : voice-only (0)
  Negotiated Codec         : g711ulaw (160 bytes)
  Codec Payload Type       : 0
  Negotiated Dtmf-relay    : inband-voice
  Dtmf-relay Payload Type  : 0
  Media Source IP Addr:Port: 172.18.19.72:17556
  Media Dest IP Addr:Port  : 172.18.19.73:17966
  Orig Media Dest IP Addr:Port : 0.0.0.0:0
  QoS ID                   : -2
  Local QoS Strength       : Optional
  Negotiated QoS Strength  : Optional
  Negotiated QoS Direction : SendRecv
  Local QoS Status         : Fail

Options-Ping    ENABLED:NO    ACTIVE:NO
   Number of SIP User Agent Server(UAS) calls: 1
```

The following is sample output from the **show sip-ua calls** command when the command is used on the originating gateway (OGW) while optional QoS is configured on the OGW, mandatory QoS is configured on the terminating gateway (TGW), and RSVP has succeeded:

```
Router# show sip-ua calls

SIP UAC CALL INFO

   Number of SIP User Agent Client(UAC) calls: 0

SIP UAS CALL INFO

Call 1
SIP Call ID              : 867EA226-D01311DC-8041CA97-F9A5F4F1@172.18.19.73
 State of the call       : STATE_ACTIVE (7)
 Substate of the call    : SUBSTATE_NONE (0)
 Calling Number          : 6001
 Called Number           : 1001
 Bit Flags               : 0x8C4401E 0x100 0x4
 CC Call ID              : 30
 Source IP Address (Sig ): 172.18.19.72
 Destn SIP Req Addr:Port : 172.18.19.73:5060
 Destn SIP Resp Addr:Port: 172.18.19.73:25055
 Destination Name        : 172.18.19.73
 Number of Media Streams : 1
 Number of Active Streams: 1
 RTP Fork Object         : 0x0
 Media Mode              : flow-through
 Media Stream 1
  State of the stream      : STREAM_ACTIVE
  Stream Call ID           : 30
```

```
  Stream Type               : voice-only (0)
  Negotiated Codec          : g711ulaw (160 bytes)
  Codec Payload Type        : 0
  Negotiated Dtmf-relay     : inband-voice
  Dtmf-relay Payload Type   : 0
  Media Source IP Addr:Port: 172.18.19.72:17556
  Media Dest IP Addr:Port   : 172.18.19.73:17966
  Orig Media Dest IP Addr:Port : 0.0.0.0:0
  QoS ID                    : -2
  Local QoS Strength        : Optional
  Negotiated QoS Strength   : Mandatory
  Negotiated QoS Direction : SendRecv
  Local QoS Status          : Success

Options-Ping    ENABLED:NO    ACTIVE:NO
   Number of SIP User Agent Server(UAS) calls: 1
```

Table 267 describes the significant fields shown in the displays.

Table 306 show sip-ua calls Field Descriptions

Field	Description
SIP UAC CALL INFO	Field header that indicates that the following information pertains to the SIP UAC.
Call 1	Field header.
SIP Call ID	UAC call identification number.
State of the call	Indicates the state of the call. This field is used for debugging purposes. The state is variable and may be different from one Cisco IOS release to another.
Substate of the call	Indicates the substate of the call. This field is used for debugging purposes. The state is variable and may be different from one Cisco IOS release to another.
Calling Number	Indicates the calling number.
Called Number	Indicates the called number.
Bit Flags	Indicates the bit flags used for debugging.
Source IP Address (Sig)	Indicates the signaling source IPv4 or IPv6 address.
Destn SIP Req Addr: Port:	Indicates the signaling destination Request IPv4 or IPv6 address and port number.
Destn SIP Resp Addr: Port:	Indicates the signaling destination Response IPv4 or IPv6 address and port number.
Destination Name	Indicates the signaling destination hostname, IPv4 address, or IPv6 address.
Number of Media Streams	Indicates the total number of media streams for this UAC call.
Number of Active Streams:	Indicates the total number of active media streams.
RTP Fork Object	Pointer address of the internal RTP Fork data structure.
Media Stream	Statistics about each active media stream are reported. The Media Stream header indicates the number of the media stream, and its statistics immediately follow this header.

Table 306 show sip-ua calls Field Descriptions (continued)

Field	Description
State of the stream	State of the media stream indicated by the Media Stream header. Can be STREAM_ACTIVE, STREAM_ADDING, STREAM_CHANGING, STREAM_DEAD, STREAM_DELETING, STREAM_IDLE, or Invalid Stream State.
Stream Call ID	Identification of the stream call indicated by the Media Stream header.
Stream Type	Type of stream indicated by the Media Stream header. It can be dtmf-only, dtmf-relay, voice-only, or voice+dtmf-relay.
Negotiated Codec	Codec selected for the media stream. It can be g711ulaw, <G.729>, <G.726>, or No Codec.
Codec Payload Type	Payload type of the Negotiated Codec.
Negotiated Dtmf-relay	DTMF relay selected for the media stream indicated by the Media Stream header. It can be inband-voice or rtp-nte.
Dtmf-relay Payload Type	Payload type of the negotiated DTMF relay.
Media Source IP Addr: Port	The source IPv4 or IPv6 address and port number of the media stream indicated by the Media Stream header.
Media Dest IP Addr: Port	The destination IPv4 or IPv6 address and port number of the media stream indicated by the Media Stream header.
Local QoS Strength	The QoS strength (mandatory or optional) configured for this device.
Negotiated QoS Strength	The QoS strength (mandatory or optional) that has been negotiated.
Negotiated QoS Direction	Displays the direction in which RSVP was negotiated. For example, sendrecv indicates that RSVP was negotiated in both directions.
Local QoS Status	Displays the success or failure of RSVP reservation.
Number of UAC calls	Final SIP UAC CALL INFO field. Indicates the number of UAC calls.
SIP UAS CALL INFO	Field header that indicates that the following information pertains to the SIP UAS.
Number of UAS calls	Final SIP UAS CALL INFO field. Indicates the number of UAS calls.

Related Commands

Command	Description
debug ccsip all	Enables all SIP-related debugging.
debug ccsip events	Enablestracing of events that are specific to SIP SPI.
debug ccsip info	Enables tracing of general SIP SPI information.
debug ccsip media	Enables tracing of SIP call media streams.
debug ccsip messages	Enables tracing of SIP Service Provider Interface (SPI) messages.

show sip-ua connections

To display Session Initiation Protocol (SIP) user-agent (UA) transport connection tables, use the **show sip-ua connections** command in privileged EXEC mode.

show sip-ua connections {**tcp** [**tls**] | **udp**} {**brief** | **detail**}

Syntax Description

tcp	Displays all TCP connection information.
tls	(Optional) Displays all Transport Layer Security (TLS) over TCP connection information.
udp	Displays all User Datagram Protocol (UDP) connection information.
brief	Displays a summary of connections.
detail	Displays detailed connection information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(8)T	This command was introduced
12.4(6)T	The optional **tls** keyword was added.
12.4(22)T	Command output was updated to show IPv6 information.
15.1(2)T	The command output was updated to display the SIP socket listeners information.

Usage Guidelines

The **show sip-ua connections** command should be executed only after a call is made. Use this command to learn the connection details.

Examples

The following sample output from this command shows multiple calls to multiple destinations. Although this example shows UDP details, the command output looks identical for TCP calls.

```
Router# show sip-ua connections udp detail

Total active connections : 2
No. of send failures : 0
No. of remote closures : 0
No. of conn. failures : 0
No. of inactive conn. ageouts : 0
---------Printing Detailed Connection Report---------
Note:
** Tuples with no matching socket entry
- Do 'clear sip <tcp/udp> conn t ipv4:<addr>:<port>'
to overcome this error condition
++ Tuples with mismatched address/port entry
- Do 'clear sip <tcp/udp> conn t ipv4:<addr>:<port> id <connid>'
to overcome this error condition
Remote-Agent:172.18.194.183, Connections-Count:1
Remote-Port Conn-Id Conn-State WriteQ-Size
```

```
=========== ======= =========== ===========
5060 1 Established 0
Remote-Agent:172.19.154.18, Connections-Count:1
Remote-Port Conn-Id Conn-State WriteQ-Size
=========== ======= =========== ===========
5060        2       Established   0

Router# show sip-ua connections tcp detail

Total active connections      : 0
No. of send failures          : 0
No. of remote closures        : 0
No. of conn. failures         : 0
No. of inactive conn. ageouts : 0
Max. tcp send msg queue size of 0, recorded for 0.0.0.0:0

---------Printing Detailed Connection Report---------
Note:
 ** Tuples with no matching socket entry
    - Do 'clear sip <tcp/udp> conn t ipv4:<addr>:<port>'
      to overcome this error condition
 ++ Tuples with mismatched address/port entry
    - Do 'clear sip <tcp/udp> conn t ipv4:<addr>:<port> id <connid>'
      to overcome this error condition

Remote-Agent:172.18.194.183, Connections-Count:1
Remote-Port Conn-Id Conn-State WriteQ-Size
=========== ======= =========== ===========
5060         1      Established   0

Router# show sip-ua connections udp detail

Total active connections      : 1
No. of send failures          : 0
No. of remote closures        : 0
No. of conn. failures         : 0
No. of inactive conn. ageouts : 0

---------Printing Detailed Connection Report---------
Note:
 ** Tuples with no matching socket entry
    - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port>'
      to overcome this error condition
 ++ Tuples with mismatched address/port entry
    - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port> id <connid>'
      to overcome this error condition

Remote-Agent:2001:DB8:C18:4:21D:E5FF:FE34:26A0, Connections-Count:1
  Remote-Port Conn-Id Conn-State  WriteQ-Size Local-Address
  =========== ======= =========== =========== ===========
         5060       2 Established           0  -

-------------- SIP Transport Layer Listen Sockets ---------------
  Conn-Id               Local-Address
 ===========    ============================
   0            [0.0.0.0]:5060
   2            [8.6.8.8]:5060

Router# show sip-ua connections tcp tls brief

Total active connections      : 0
No. of send failures          : 0
No. of remote closures        : 0
No. of conn. failures         : 0
```

```
No. of inactive conn. ageouts : 0
TLS client handshake failures : 0
TLS server handshake failures : 0

-------------- SIP Transport Layer Listen Sockets ---------------
  Conn-Id               Local-Address
 ===========    ============================
   0            [0.0.0.0]:5061
```

The following is sample output from the **show sip-ua connections** command showing IPv6 information:

```
Router# show sip-ua connections udp brief

Total active connections      : 0
No. of send failures          : 0
No. of remote closures        : 0
No. of conn. failures         : 0
No. of inactive conn. ageouts : 10

-------------- SIP Transport Layer Listen Sockets ---------------
  Conn-Id               Local-Address
 ===========    ============================
   0            [0.0.0.0]:5060
```

Table 307 describes the significant fields shown in the display.

Table 307 show sip-ua connections Field Descriptions

Field	Description
Total active connections	Indicates all the connections that the gateway holds for various targets. Statistics are broken down within individual fields.
No. of send failures	Indicates the number of TCP or UDP messages dropped by the transport layer. Messages are dropped if there were network issues, and the connection was frequently ended.
No. of remote closures	Indicates the number of times a remote gateway ended the connection. A higher value indicates a problem with the network or that the remote gateway does not support reusing the connections (thus it is not RFC 3261-compliant). The remote closure number can also contribute to the number of send failures.
No. of conn. failures	Indicates the number of times that the transport layer was unsuccessful in establishing the connection to the remote agent. The field can also indicate that the address or port configured under the dial peer might be incorrect or that the remote gateway does not support that mode of transport.
No. of inactive conn. ageouts	Indicates the number of times that the connections were ended or timed out because of signaling inactivity. During call traffic, this number should be zero. If it is not zero, we recommend that the inactivity timer be tuned to optimize performance by using the **timers** command.
Max. tcp send msg queue size of 0, recorded for 0.0.0.0:0	Indicates the number of messages waiting in the queue to be sent out on the TCP connection when the congestion was at its peak. A higher queue number indicates that more messages are waiting to be sent on the network. The growth of this queue size cannot be controlled directly by the administrator.

Table 307 show sip-ua connections Field Descriptions (continued)

Field	Description
Tuples with no matching socket entry	Any tuples for the connection entry that are marked with "**" at the end of the line indicate an upper transport layer error condition; specifically, that the upper transport layer is out of sync with the lower connection layer. Cisco IOS software should automatically overcome this condition. If the error persists, execute the **clear sip-ua udp connection** or **clear sip-ua tcp connection** command and report the problem to your support team.
Tuples with mismatched address/port entry	Any tuples for the connection entry that are marked with "++" at the end of the line indicate an upper transport layer error condition, where the socket is probably readable, but is not being used. If the error persists, execute the **clear sip-ua udp connection** or **clear sip-ua tcp connection** command and report the problem to your support team.
Remote-Agent Connections-Count	Connections to the same target address. This field indicates how many connections are established to the same host.
Remote-Port Conn-Id Conn-State WriteQ-Size	Connections to the same target address. This field indicates how many connections are established to the same host. The WriteQ-Size field is relevant only to TCP connections and is a good indicator of network congestion and if there is a need to tune the TCP parameters.

Related Commands

Command	Description
clear sip-ua tcp connection	Clears a SIP TCP connection.
clear sip-ua udp connection	Clears a SIP UDP connection.
show sip-ua retry	Displays SIP retry statistics.
show sip-ua statistics	Displays response, traffic, and retry SIP statistics.
show sip-ua status	Displays SIP user agent status.
show sip-ua timers	Displays the current settings for the SIP UA timers.
sip-ua	Enables the SIP user-agent configuration commands.
timers	Configures the SIP signaling timers.

show sip-ua status

To display status for the Session Initiation Protocol (SIP) user agent (UA), use the **show sip-ua status** command in privileged EXEC mode.

show sip-ua status

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.1(3)T	The statistics portion of the output was removed and included in the **show sip-ua statistics** command.
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB	Command output was enhanced to display if media or signaling binding is enabled, and the style of the DNS SRV query (1 for RFC 2052; 2 for RFC 2782).
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 was not included in this release. For the purposes of display, this command was separated from the generic **show sip-ua** command.
12.2(11)T	Command output was enhanced to display information on Session Description Protocol (SDP) application configuration. This command was supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.
12.2(13)T	Command output was enhanced to display the following: Information on redirection message handling. Information on handling of 180 responses with SDP.
12.2(15)T	Command output was enhanced to display Suspend and Resume support.
12.2(15)ZJ	Command output was enhanced to display information on the duration of dual-tone multifrequency (DTMF) events.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.3(8)T	Command output was enhanced to display Reason Header support.
12.4(22)T	Command output was updated to show IPv6 information.
Cisco IOS Release XE 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

Use this command to verify SIP configurations.

Examples

The following is sample output from the **show sip-ua status** command:

```
Router# show sip-ua status

SIP User Agent Status
SIP User Agent for UDP : ENABLED
SIP User Agent for TCP : ENABLED

SIP User Agent for TLS over TCP : ENABLED
SIP User Agent bind status(signaling): DISABLED
SIP User Agent bind status(media): DISABLED
SIP early-media for 180 responses with SDP: ENABLED
SIP max-forwards : 70
SIP DNS SRV version: 2 (rfc 2782)
NAT Settings for the SIP-UA
Role in SDP: NONE
Check media source packets: DISABLED
Maximum duration for a telephone-event in NOTIFYs: 2000 ms
SIP support for ISDN SUSPEND/RESUME: ENABLED
Redirection (3xx) message handling: ENABLED
Reason Header will override Response/Request Codes: DISABLED
Out-of-dialog Refer: DISABLED
Presence support is DISABLED
protocol mode is ipv4

SDP application configuration:
 Version line (v=) required
 Owner line (o=) required
 Timespec line (t=) required
 Media supported: audio video image
 Network types supported: IN
 Address types supported: IP4 IP6
 Transport types supported: RTP/AVP udptl
```

The following is sample output from the **show sip-ua status** command showing IPv6 information:

```
Router# show sip-ua status

SIP User Agent Status
SIP User Agent for UDP : ENABLED
SIP User Agent for TCP : ENABLED

SIP User Agent for TLS over TCP : ENABLED
SIP User Agent bind status(signaling): DISABLED
SIP User Agent bind status(media): DISABLED
SIP early-media for 180 responses with SDP: ENABLED
SIP max-forwards : 70
SIP DNS SRV version: 2 (rfc 2782)
NAT Settings for the SIP-UA
Role in SDP: NONE
Check media source packets: DISABLED
Maximum duration for a telephone-event in NOTIFYs: 2000 ms
SIP support for ISDN SUSPEND/RESUME: ENABLED
Redirection (3xx) message handling: ENABLED
Reason Header will override Response/Request Codes: DISABLED
Out-of-dialog Refer: DISABLED
Presence support is DISABLED
protocol mode is ipv6

SDP application configuration:
 Version line (v=) required
Owner line (o=) required
 Timespec line (t=) required
 Media supported: audio video image
```

```
Network types supported: IN
Address types supported: IP4 IP6
Transport types supported: RTP/AVP udptl
```

Table 308 describes the significant fields shown in the display.

Table 308 show sip-ua status Field Descriptions

Field	Description
SIP User Agent Status	UA status.
SIP User Agent for UDP	User Datagram Protocol (UDP) is enabled or disabled.
SIP User Agent for TCP	TCP is enabled or disabled.
SIP User Agent bind status (signaling)	Binding for signaling is enabled or disabled.
SIP User Agent bind status (media)	Binding for media is enabled or disabled.
SIP early-media for 180 responses with SDP	Early media cut-through treatment for 180 responses with SDP can be enabled (the default treatment) or disabled, with local ringback provided.
SIP max-forwards	Value of max-forwards of SIP messages.
SIP DNS SRV version	Style of the DNS SRV query: 1 for RFC 2052 or 2 for RFC 2782.
NAT Settings for the SIP-UA	Symmetric Network Address Translation (NAT) settings when the feature is enabled.
Role in SDP	Identifies the endpoint function in the connection setup procedure during symmetric NAT traversal. The endpoint role may be set to active, meaning that it initiates a connection, or to passive, meaning that it accepts a connection. A value of none in this field means that the feature is disabled.
Check media source packets	Media source packet checking is enabled or disabled.
Maximum duration for a telephone-event in NOTIFYs	Shows the time interval, in milliseconds (ms), between consecutive NOTIFY messages for a telephone event.
SIP support for ISDN SUSPEND/RESUME	Suspend and Resume support is enabled or disabled.
Redirection (3xx) message handling	Redirection can be enabled, which is the default status, according to RFC 2543. Or handling of redirection 3*xx* messages can be disabled, allowing the gateway to treat 3*xx* redirect messages as 4*xx* error messages.
Reason Header will override Response/Request Codes	Reason header is enabled or disabled.
protocol mode is ipv6	States whether the protocol being used is IPv6 or IPv4.
Version line (v=)	Indicates if the SDP version is required.
Owner line (o=)	Indicates if the session originator is required.
Timespec line (t=)	Indicates if the session start and stop times are required.
Media supported	Media information.
Network types supported	Always IN for Internet.

Table 308 show sip-ua status Field Descriptions (continued)

Field	Description
Address types supported	Identifies the Internet Protocol version.
Transport types supported	Identifies the transport protocols supported.

Related Commands

Command	Description
show sip-ua retry	Displays SIP retry statistics.
show sip-ua statistics	Displays response, traffic, and retry SIP statistics.
show sip-ua timers	Displays the current settings for SIP UA timers.
sip-ua	Enables the SIP user-agent configuration commands.

show standby

To display Hot Standby Router Protocol (HSRP) information, use the **show standby** command in user EXEC or privileged EXEC mode.

show standby [*type number* [*group*]] [**all** | **brief**]

Syntax Description

type number	(Optional) Interface type and number for which output is displayed.
group	(Optional) Group number on the interface for which output is displayed.
all	(Optional) Displays information for groups that are learned or do not have the **standby ip** command configured.
brief	(Optional) A single line of output summarizes each standby group.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.2(8)T	The output for the command was made clearer and easier to understand.
12.3(2)T	The output was enhanced to display information about Message Digest 5 (MD5) authentication.
12.3(4)T	The output was enhanced to display information about HSRP version 2.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.4(4)T	IPv6 support was added.
12.4(6)T	The output for this command was enhanced to display information about HSRP master and client groups.
12.4(9)T	The output for this command was enhanced to display information about HSRP group shutdown configuration.
12.4(11)T	The output for this command was enhanced to display information about HSRP Bidirectional Forwarding Detection (BFD) peering.
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.
12.2(33)SXI	The output for this command was enhanced to display information about gratuitous ARP packets.
12.4(24)T	This command was modified. The output was modified to hide configured passwords when MD5 key-string or text authentication is configured.
12.2(33)SXI1	This command was modified. The output was modified to hide configured passwords when MD5 key-string or text authentication is configured.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Release	Modification
Cisco IOS XE Release 2.4	This command was modified. The output was modified to hide configured passwords when MD5 key-string or text authentication is configured.
12.2(33)SRE	This command was modified. The output was modified to hide configured passwords when MD5 key-string or text authentication is configured.

Usage Guidelines

To specify a group, you must specify an interface type and number.

Examples

The following is sample output from the **show standby** command:

```
Router# show standby

Ethernet0/1 - Group 1
  State is Active
   2 state changes, last state change 00:30:59
  Virtual IP address is 10.1.0.20
   Secondary virtual IP address 10.1.0.21
  Active virtual MAC address is 0004.4d82.7981
   Local virtual MAC address is 0004.4d82.7981 (bia)
  Hello time 4 sec, hold time 12 sec
   Next hello sent in 1.412 secs
  Gratuitous ARP 14 sent, next in 7.412 secs
  Preemption enabled, min delay 50 sec, sync delay 40 sec
  Active router is local
  Standby router is 10.1.0.6, priority 75 (expires in 9.184 sec)
  Priority 95 (configured 120)
   Tracking 2 objects, 0 up
      Down Interface Ethernet0/2, pri 15
      Down Interface Ethernet0/3
Group name is "HSRP1" (cfgd)
Follow by groups:
    Et1/0.3 Grp 2 Active 10.0.0.254 0000.0c07.ac02 refresh 30 secs (next 19.666)
    Et1/0.4 Grp 2 Active 10.0.0.254 0000.0c07.ac02 refresh 30 secs (next 19.491)
  Group name is "HSRP1", advertisement interval is 34 sec
```

The following is sample output from the **show standby** command when HSRP version 2 is configured:

```
Router# show standby

Ethernet0/1 - Group 1 (version 2)
  State is Speak
  Virtual IP address is 10.21.0.10
  Active virtual MAC address is unknown
   Local virtual MAC address is 0000.0c9f.f001 (v2 default)
  Hello time 3 sec, hold time 10 sec
   Next hello sent in 1.804 secs

  Preemption enabled
  Active router is unknown
  Standby router is unknown
  Priority 20 (configured 20)
  Group name is "hsrp-Et0/1-1" (default)

Ethernet0/2 - Group 1
  State is Speak
  Virtual IP address is 10.22.0.10
  Active virtual MAC address is unknown
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
```

```
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.804 secs
  Preemption disabled
  Active router is unknown
  Standby router is unknown
  Priority 90 (default 100)
    Track interface Serial2/0 state Down decrement 10
  Group name is "hsrp-Et0/2-1" (default)
```

The following is sample output from the **show standby** command with the **brief** keyword specified:

```
Router# show standby brief

Interface   Grp Prio P State    Active addr     Standby addr    Group addr
Et0         0   120    Init     10.0.0.1        unknown         10.0.0.12
```

The following is sample output from the **show standby** command when HSRP MD5 authentication is configured:

```
Router# show standby

Ethernet0/1 - Group 1
  State is Active
    5 state changes, last state change 00:17:27
  Virtual IP address is 10.21.0.10
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.276 secs
  Authentication MD5, key-string, timeout 30 secs
  Preemption enabled
  Active router is local
  Standby router is unknown
  Priority 110 (configured 110)
  Group name is "hsrp-Et0/1-1" (default)
```

The following is sample output from the **show standby** command when HSRP group shutdown is configured:

```
Router# show standby

Ethernet0/0 - Group 1
State is Init (tracking shutdown)
3 state changes, last state change 00:30:59
Track object 100 state Up
Track object 101 state Down
Track object 103 state Up
```

The following is sample output from the **show standby** command when HSRP BFD peering is enabled:

```
Router# show standby

Ethernet0/0 - Group 2
  State is Listen
    2 state changes, last state change 01:18:18
  Virtual IP address is 10.0.0.1
  Active virtual MAC address is 0000.0c07.ac02
    Local virtual MAC address is 0000.0c07.ac02 (v1 default)
  Hello time 3 sec, hold time 10 sec
  Preemption enabled
  Active router is 10.0.0.250, priority 120 (expires in 9.396 sec)
  Standby router is 10.0.0.251, priority 110 (expires in 8.672 sec)
    BFD enabled
  Priority 90 (configured 90)
```

```
  Group name is "hsrp-Et0/0-1" (default)
```

The following is sample output from the **show standby** command used to display the state of the standby RP:

```
Router# show standby

GigabitEthernet3/25 - Group 1
State is Init (standby RP, peer state is Active)
Virtual IP address is 10.0.0.1
Active virtual MAC address is unknown
Local virtual MAC address is 0000.0c07.ac01 (v1 default)
Hello time 3 sec, hold time 10 sec
Preemption disabled
Active router is unknown
Standby router is unknown
Priority 100 (default 100)
Group name is "hsrp-Gi3/25-1" (default)
```

Table 309 describes the significant fields shown in the displays.

Table 309 show standby Field Descriptions

Field	Description
Ethernet - Group	Interface type and number and Hot Standby group number for the interface.
State is	State of local router; can be one of the following: • Active—Indicates the current Hot Standby router. • Standby—Indicates the router next in line to be the Hot Standby router. • Speak—Router is sending packets to claim the active or standby role. • Listen—Router is neither in the active nor standby state, but if no messages are received from the active or standby router, it will start to speak. • Init or Disabled—Router is not yet ready or able to participate in HSRP, possibly because the associated interface is not up. HSRP groups configured on other routers on the network that are learned via snooping are displayed as being in the Init state. Locally configured groups with an interface that is down or groups without a specified interface IP address appear in the Init state. For these cases, the Active addr and Standby addr fields will show "unknown." The state is listed as disabled in the fields when the **standby ip** command has not been specified. • Init (tracking shutdown)—HSRP groups appear in the Init state when HSRP group shutdown has been configured and a tracked object goes down.
Virtual IP address is, Secondary virtual IP addresses	All secondary virtual IP addresses are listed on separate lines. If one of the virtual IP addresses is a duplicate of an address configured for another device, it will be marked as "duplicate." A duplicate address indicates that the router has failed to defend its ARP (Address Resolution Protocol) cache entry.
Active virtual MAC address	Virtual MAC address being used by the current active router.
Local virtual MAC address	Virtual MAC address that would be used if this router became the active router. The origin of this address (displayed in parentheses) can be "default," "bia," (burned-in address) or "confgd" (configured).

Table 309 show standby Field Descriptions (continued)

Field	Description
Hello time, hold time	The hello time is the time between hello packets (in seconds) based on the command. The holdtime is the time (in seconds) before other routers declare the active or standby router to be down, based on the **standby timers** command. All routers in an HSRP group use the hello and hold- time values of the current active router. If the locally configured values are different, the variance appears in parentheses after the hello time and hold-time values.
Next hello sent in	Time in which the Cisco IOS software will send the next hello packet (in hours:minutes:seconds).
Gratuitous ARP 14 sent, next in 7.412 secs	Number of the gratuitous ARP packet HSRP has sent and the time in seconds when HSRP will send the next gratuitous ARP packet. This output appears only when HSRP sends gratuitous ARP packets.
Authentication	Authentication type configured based on the **standby authentication** command.
key-string	Indicates a key string is used for authentication. Configured key chains are not displayed.
timeout	Duration (in seconds) that HSRP will accept message digests based on both the old and new keys.
Preemption enabled, sync delay	Indicates whether preemption is enabled. If enabled, the minimum delay is the time a higher-priority nonactive router will wait before preempting the lower-priority active router. The sync delay is the maximum time a group will wait to synchronize with the IP redundancy clients.
Active router is	Value can be “local,” “unknown,” or an IP address. Address (and the expiration date of the address) of the current active Hot Standby router.
Standby router is	Value can be “local,” “unknown,” or an IP address. Address (and the expiration date of the address) of the “standby” router (the router that is next in line to be the Hot Standby router).
BFD enabled	Indicates that BFD peering is enabled on the router.
expires in	Time (in hours:minutes:seconds) in which the standby router will no longer be the standby router if the local router receives no hello packets from it.
Tracking	List of interfaces that are being tracked and their corresponding states. Based on the **standby track** command.
Group name is	The name of the HSRP group.
Follow by groups:	Indicates the client HSRP groups that have been configured to follow this HSRP group.
P	Indicates that the router is configured to preempt.

Related Commands

Command	Description
standby authentication	Configures an authentication string for the HSRP.
standby ip	Activates the HSRP.
standby mac-address	Specifies the virtual MAC address for the virtual router.
standby mac-refresh	Refreshes the MAC cache on the switch by periodically sending packets from the virtual MAC address.

Command	Description
standby preempt	Configures HSRP preemption and preemption delay.
standby priority	Configures Hot Standby priority of potential standby routers.
standby timers	Configures the time between hello messages and the time before other routers declare the active Hot Standby or standby router to be down.
standby track	Configures an interface so that the Hot Standby priority changes based on the availability of other interfaces.
standby use-bias	Configures HSRP to use the BIA of the interface as its virtual MAC address, instead of the preassigned MAC address (on Ethernet and FDDI) or the functional address (on Token Ring).

show stcapp device

To display configuration information about Skinny Client Control Protocol (SCCP) telephony control (STC) application (STCAPP) analog voice ports, use the **show stcapp device** command in privileged EXEC mode.

show stcapp device {**name** *device-name* | **summary** | **voice-port** *port*}

Syntax Description

name *device-name*	Displays information for the analog voice port with the specified device name. The device name is the unique device ID that is assigned to the port when it registers with the call-control system.
summary	Displays a summary of all voice ports.
voice-port *port*	Displays information for the specified analog voice port. **Note** The *port* syntax is platform-dependent; type ? to determine appropriate port numbering.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(2)T	This command was modified. Command output was enhanced to display call control block (CCB) and call-control device information.
12.4(4)T	This command was modified. Command output was enhanced to display supported modem transport capability.
12.4(6)XE	This command was modified. Command output was enhanced to display visual message waiting indicator (VMWI) and information for Dial Tone After Remote Onhook feature.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.4(22)T	This command was modified. Command output was updated to show IPv6 information.
15.0(1)XA	This command was modified. Cancel Call Waiting information was added to the command output.
15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.
15.1(3)T	This command was modified. Command output was enhanced to display the call waiting tone configuration.

Usage Guidelines

Use this command to display configuration and voice interface card (VIC)-specific port information. The Active Call Info field is populated only if a call is active on the voice port.

Examples

The following is a sample output showing IPv6 addresses for the local and remote sites:

```
Router# show stcapp device voice-port 2/0

Port Identifier: 2/0
Device Type: ALG
Device Id: 1
Device Name: AN1AE2853624400
Device Security Mode : None
Modem Capability: None
Device State: IS
Diagnostic: None
Directory Number: 1000
Dial Peer(s): 1000
Dialtone after remote onhook feature: activated
Busytone after remote onhook feature: not activated
Last Event: STCAPP_DC_EV_DEVICE_CALL_INFO
Line State: ACTIVE
Hook State: OFFHOOK
mwi: DISABLE
vmwi: OFF
PLAR: DISABLE
Number of CCBs: 1
Global call info:
Total CCB count = 2
Total call leg count = 4

Call State for Connection 1: TsConnected
Connected Call Info:
Call Reference: 22690511
Local IPv6 Addr: 2001:DB8:C18:1:218:FEFF:FE71:2AB6
Local IP Port: 17424
Remote IPv6 Addr: 2001:DB8:C18:1:218:FEFF:FE71:2AB6
Remote IP Port: 18282
Calling Number: 1000
Called Number:
Codec: g729br8
SRTP: off
```

The following is a sample output from the **show stcapp device** command for an SCCP analog port with VMWI while the Dial Tone After Remote Onhook Feature is activated:

```
Router# show stcapp device voice-port 2/4
Port Identifier:  2/4
Device Type:      ALG
Device Id:        4
Device Name:      AN0C863967C9404
Modem Capability: None
Device State:     IS
Diagnostic:       None
Directory Number: 7204
Dial Peer(s):     4
Dialtone after remote onhook feature: activated
Last Event:       STCAPP_CC_EV_CALL_DISCONNECT_DONE
Line State:       IDLE
Hook State:       ONHOOK
mwi:              ENABLE
vmwi:             ON
PLAR:             DISABLE
Number of CCBs:   0
```

The following is a sample output from the **show stcapp device** command for an STCAPP analog voice port on a VIC2-2FXS voice interface card specified by the port number:

```
Router# show stcapp device voice-port 1/0/0

Port Identifier:  1/0/0
Device Type:      ALG
Device Id:        3
Device Name:      AN1EBEEB6070200
Device Security Mode : None
Modem Capability: None
Device State:     IS
Diagnostic:       None
Directory Number: 2099
Dial Peer(s):     999100
Dialtone after remote onhook feature: activated
Busytone after remote onhook feature: not activated
Last Event:       STCAPP_CC_EV_CALL_DISCONNECT_DONE
Line State:       IDLE
Line Mode:        CALL_BASIC
Hook State:       ONHOOK
ccw_on:           FALSE
mwi:              DISABLE
vmwi:             OFF
PLAR:             DISABLE
Callback State:   DISABLED
Number of CCBs:   0
Global call info:
    Total CCB count      = 0
    Total call leg count = 0
```

The following is a sample output from the **show stcapp device** command for an STCAPP analog voice port:

```
Router# show stcapp device name AN0C863972F5401

Port Identifier:  2/1
Device Type:      ALG
Device Id:        25
Device Name:      AN0C863972F5401
Device State:     IS
Diagnostic:       None
Directory Number: 9101
Dial Peer(s):     2
Last Event:       STCAPP_CC_EV_CALL_MODIFY_DONE
Line State:       ACTIVE
Hook State:       OFFHOOK
Number of CCBs:   1
Global call info:
    Total CCB count      = 3
    Total call leg count = 6

Call State for Connection 1: TsConnected
Connected Call Info:
   Call Reference: 16777509
   Local IP Addr:  10.1.0.1
   Local IP Port:  18768
   Remote IP Addr: 10.1.0.1
   Remote IP Port: 18542
   Calling Number: 9101
   Called Number:  9102
   Codec:          g711ulaw
```

The following is a sample output from the **show stcapp device** command for STCAPP analog voice ports:

```
Router# show stcapp device summary

Total Devices:           24
Total Calls in Progress: 3
Total Call Legs in Use:  6

Port       Device          Device   Call          Dev  Directory   Dev
Identifier Name            State    State         Type Number      Cntl
---------- --------------- -------- ------------- ---- ----------- ----
2/1        AN0C863972F5401 IS       ACTIVE         ALG  9101       CCM
2/2        AN0C863972F5402 IS       ACTIVE         ALG  9102       CCM
2/3        AN0C863972F5403 IS       ACTIVE         ALG  9103       CCM
2/0        AN0C863972F5400 IS       IDLE           ALG  9100       CCM
2/4        AN0C863972F5404 IS       IDLE           ALG  9104       CCM
2/5        AN0C863972F5405 IS       IDLE           ALG  9105       CCM
2/6        AN0C863972F5406 IS       IDLE           ALG  9106       CCM
2/7        AN0C863972F5407 IS       IDLE           ALG  9107       CCM
2/8        AN0C863972F5408 IS       IDLE           ALG  9108       CCM
2/9        AN0C863972F5409 IS       IDLE           ALG  9109       CCM
2/10       AN0C863972F540A IS       IDLE           ALG  9110       CCM
2/11       AN0C863972F540B IS       IDLE           ALG  9111       CCM
2/12       AN0C863972F540C IS       IDLE           ALG  9112       CCM
2/13       AN0C863972F540D IS       IDLE           ALG  9113       CCM
2/14       AN0C863972F540E IS       IDLE           ALG  9114       CCM
2/15       AN0C863972F540F IS       IDLE           ALG  9115       CCM
2/16       AN0C863972F5410 IS       IDLE           ALG  9116       CCM
2/17       AN0C863972F5411 IS       IDLE           ALG  9117       CCM
2/18       AN0C863972F5412 IS       IDLE           ALG  9118       CCM
2/19       AN0C863972F5413 IS       IDLE           ALG  9119       CCM
2/20       AN0C863972F5414 IS       IDLE           ALG  9120       CCM
2/21       AN0C863972F5415 IS       IDLE           ALG  9121       CCM
2/22       AN0C863972F5416 IS       IDLE           ALG  9122       CCM
2/23       AN0C863972F5417 IS       IDLE           ALG  9123       CCM
```

The following is a sample output from the **show stcapp device** command for an STCAPP analog voice port:

```
Router# show stcapp device name AN0C86385E3D400

Port Identifier: 2/0
Device Type:      ALG
Device Id:        1
Device Name:      AN0C86385E3D400
Device Security Mode : None
Modem Capability: None
Device State:     IS
Diagnostic:       None
Directory Number: 2400
Dial Peer(s):     2000
Dialtone after remote onhook feature: activated
Busytone after remote onhook feature: not activated
Last Event:       STCAPP_DC_EV_DEVICE_DISPLAY_PROMPT_STATUS
Line State:       IDLE
Line Mode:        CALL_BASIC
Hook State:       ONHOOK
mwi:              DISABLE
vmwi:             OFF
mwi config:       Both
Privacy:          Not configured
PLAR:             DISABLE
Callback State:   IDLE
```

```
CWT Repetition Interval: 0 second(s)
Number of CCBs:   0
Global call info:
    Total CCB count      = 0
    Total call leg count = 0
```

Table 310 describes the significant fields shown in these displays, in alphabetical order.

Table 310 show stcapp device Field Descriptions

Field	Description
Active Call Info	Displays only when an active call is in progress.
Call Reference	Reference number created by Cisco Unified Communications Manager to track messages associated with a specific call.
Call State	Call processing state: • ACTIVE—Established call connection • IDLE—No call connection • UNREGISTERED—Device is not registered with the Cisco Unified Communications Manager
Called Number	Device called number.
Calling Number	Device calling number.
ccw_on	Displays status of Cancel Call Waiting feature: • False—Inactive on port. • True—Active on port.
Codec	Displays codec type.
CWT Repetition Interval	Displays the call waiting tone configuration.
Dev Cntl	Call-control device that is managing the analog endpoints. CCM represents Cisco Unified Communications Manager. CME represents Cisco Unified Communications Manager Express.
Device Id	Identifier used between the Cisco Unified Communications Manager and gateway to uniquely identify an endpoint.
Device Name	Unique device ID of the analog endpoint. The device ID is derived from an algorithm using the MAC address of the SCCP interface on the voice gateway and the hexadecimal translation of the port's slot number and port number.

Table 310 show stcapp device Field Descriptions (continued)

Field	Description
Device State	Displays whether device is available for use: • ACTIVE_PENDING—Call is pending certain events before going active. • INFO_RCVD—Call information is received from the Cisco Unified Communications Manager during call setup. • INIT—Waiting to reinitialize. • IS—In service. • OFFHOOK—Device is off-hook. • OFFHOOK_TIMEOUT—Digit timeout occurred while the device is off-hook. • ONHOOK_PENDING—Call is pending certain events before going to the on-hook state. • OOS—Out of service. • PROCEED—Dialed number translation is complete and call setup is in progress. • REM_ONHOOK_PENDING—Call is pending certain events before going to the on-hook state. • RINGING—An incoming call has invoked ringing of the receiving device.
Device Type	Shows phone type: • ALG—Analog. • BRI—ISDN BRI.
Diagnostic	Reason code for a device error condition.
Dial Peer(s)	Dial peer name.
Dialtone after remote onhook feature	Displays feature status: • Activated • Not activated
Directory Number	Assigned to the device by the Cisco Unified Communications Manager.
Last Event	Last event processed by this port.
Local IP Addr	IPv4 address of this gateway used to stream audio using the Real-Time Transport Protocol (RTP).
Local IPv6 Addr	IPv6 address of this gateway used to stream audio using the RTP.
Local IP Port	IP port of this gateway used to stream audio using RTP.
Port Identifier	Identifies the physical voice port.
Remote IP Addr	IPv4 address of the far-end gateway that streams audio using RTP.
Remote IPv6 Addr	IPv6 address of the far-end gateway that streams audio using RTP.

Table 310 show stcapp device Field Descriptions (continued)

Field	Description
Remote IP Port	IP port of the far-end gateway that streams audio using RTP.
vmwi	Displays LED status: • On • Off

Related Commands

Command	Description
show stcapp statistics	Displays call statistics for STCAPP devices.

show trace multilink

To display information about multilink Frame Relay (MFR) issues, use the s**how trace multilink** command in privileged EXEC mode.

show trace multilink [**clear** | **continuous** | **detail** | **display** | **filter** | **last** | **resume** | **size** | **stop**]

Syntax Description

clear	(Optional) Value used to clear the trace buffer.
continuous	(Optional) Value that allows the trace to be shown continuously.
detail	(Optional) Value that provides trace detail.
display	(Optional) Value that control display options.
filter	(Optional) Value used to specify a filter.
last	(Optional) Value used to display the last several issues.
resume	(Optional) Value used to resume tracing.
size	(Optional) Trace buffer size, in bytes.
stop	(Optional) Value used to stop tracing.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(33)S	This command was introduced on the Cisco 12000 Series Routers.

Usage Guidelines

The **show trace multilink** command is useful in tracking what events happened when multilink Frame Relay goes up or goes down. The CLI is a debug tool used to collect the event logs pertaining to multilink feature. This command can be issued on the Router Processor Card (RP) and on individual line cards (LC) in the Cisco IOS 12000 series.

Examples

The following example enables the **show trace multilink** command:

```
Router# show trace multilink
```

show track

To display information about objects that are tracked by the tracking process, use the **show track** command in privileged EXEC mode.

show track [*object-number* [**brief**] | **interface** [**brief**] | **ip route** [**brief**] | **resolution** | **timers**]

Syntax Description

object-number	(Optional) Object number that represents the object to be tracked. The range is from 1 to 1000.
brief	(Optional) Displays a single line of information related to the preceding argument or keyword.
interface	(Optional) Displays tracked interface objects.
ip route	(Optional) Displays tracked IP-route objects.
resolution	(Optional) Displays resolution of tracked parameters.
timers	(Optional) Displays polling interval timers.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.3(8)T	The output was enhanced to include the track-list objects.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.4(2)T	The output was enhanced to display stub objects.
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(9)T	This command was enhanced to display information about the status of an interface when carrier-delay detection has been enabled.
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.
12.4(20)T	The output was enhanced to display IP SLAs information.
15.1(3)T	This command was modified. The valid range of the *object-number* argument increased to 1000.
15.1(1)S	This command was modified. The valid range for the *object-number* argument increased to 1000.

Usage Guidelines

Use this command to display information about objects that are tracked by the tracking process. When no arguments or keywords are specified, information for all objects is displayed.

As of Cisco IOS Release 15.1(3)T, a maximum of 1000 objects can be tracked. Although 1000 tracked objects can be configured, each tracked object uses CPU resources. The amount of available CPU resources on a router is dependent upon variables such as traffic load and how other protocols are configured and run. The ability to use 1000 tracked objects is dependent upon the available CPU. Testing should be conducted on site to ensure that the service works under the specific site traffic conditions.

Examples

The following example shows information about the state of IP routing on the interface that is being tracked:

```
Router# show track 1

Track 1
 Interface Ethernet0/2 ip routing
 IP routing is Down (no IP addr)
  1 change, last change 00:01:08
 Tracked by:
  HSRP Ethernet0/3 1
```

The following example shows information about the line-protocol state on the interface that is being tracked:

```
Router# show track 1

Track 1
 Interface Ethernet0/1 line-protocol
 Line protocol is Up
  1 change, last change 00:00:05
 Tracked by:
  HSRP Ethernet0/3 1
```

The following example shows information about the reachability of a route that is being tracked:

```
Router# show track 1

Track 1
 IP route 10.16.0.0 255.255.0.0 reachability
 Reachability is Up (RIP)
  1 change, last change 00:02:04
 First-hop interface is Ethernet0/1
 Tracked by:
  HSRP Ethernet0/3 1
```

The following example shows information about the threshold metric of a route that is being tracked:

```
Router# show track 1

Track 1
 IP route 10.16.0.0 255.255.0.0 metric threshold
 Metric threshold is Up (RIP/6/102)
  1 change, last change 00:00:08
 Metric threshold down 255 up 254
 First-hop interface is Ethernet0/1
 Tracked by:
  HSRP Ethernet0/3 1
```

The following example shows the object type, the interval in which it is polled, and the time until the next poll:

```
Router# show track timers

 Object type   Poll Interval  Time to next poll
 interface     1              expired
```

```
 ip route      30             29.364
```

The following example shows the state of the IP SLAs tracking:

```
Router# show track 50

Track 50
  IP SLA 400 state
  State is Up
    1 change, last change 00:00:23
  Delay up 60 secs, down 30 secs
  Latest operation return code: Unknown
```

The following example shows whether a route is reachable:

```
Router# show track 3

Track 3
   IP SLA 1 reachability
   Reachability is Up
     1 change, last change 00:00:47
   Latest operation return code: over threshold
   Latest RTT (millisecs) 4
   Tracked by:
     HSRP Ethernet0/1 3
```

Table 311 describes the significant fields shown in the displays.

Table 311 show track Field Descriptions

Field	Description
Track	Object number that is being tracked.
Interface Ethernet0/2 ip routing	Interface type, interface number, and object that is being tracked.
IP routing is	State value of the object, displayed as Up or Down. If the object is down, the reason is displayed.
1 change, last change	Number of times that the state of a tracked object has changed and the time (in *hh:mm:ss*) since the last change.
Tracked by	Client process that is tracking the object.
First-hop interface is	Displays the first-hop interface.
Object type	Object type that is being tracked.
Poll Interval	Interval (in seconds) in which the tracking process polls the object.
Time to next poll	Period of time, in seconds, until the next polling of the object.

The following output shows that there are two objects. Object 1 has been configured with a weight of 10 “down,” and object 2 has been configured with a weight of 20 “up.” Object 1 is down (expressed as 0/10) and object 2 is up. The total weight of the tracked list is 20 with a maximum of 30 (expressed as 20/30). The “up” threshold is 20, so the list is “up.”

```
Router# show track

 Track 6
 List threshold weight
  Threshold weight is Up (20/30)
   1 change, last change 00:00:08
```

```
   object 1 Down (0/10)
   object 2 weight 20 Up (20/30)
  Threshold weight down 10 up 20
   Tracked by:
    HSRP Ethernet0/3 1
```

The following example shows information about the Boolean configuration:

```
Router# show track

 Track 3
 List boolean and
 Boolean AND is Down
  1 change, last change 00:00:08
   object 1 not Up
   object 2 Down
 Tracked by:
  HSRP Ethernet0/3 1
```

Table 312 describes the significant fields shown in the displays.

Table 312 show track Field Descriptions

Field	Description
Track	Object number that is being tracked.
Boolean AND is Down	Each object defined in the list must be in a down state.
1 change, last change	Number of times that the state of a tracked object has changed and the time (in *hh:mm:ss*) since the last change.
Tracked by	Client process that is tracking the object; in this case, HSRP.

The following example shows information about a stub object that has been created to be tracked using Embedded Event Manager (EEM):

```
Router# show track

Track 1
  Stub-object
  State is Up
    1 change, last change 00:00:04, by Undefined
```

The following example shows information about a stub object when the **brief** keyword is used:

```
Router# show track brief

Track   Object                          Parameter        Value Last Change
1       Stub-object Undefined                            Up    00:00:12
```

The following example shows information about the line-protocol state on an interface that is being tracked and which has carrier-delay detection enabled:

```
Router# show track

Track 101
Interface Ethernet1/0 line-protocol
Line protocol is Down (carrier-delay)
1 change, last change 00:00:03
```

Table 313 describes the significant fields shown in the displays.

Table 313 show track brief Field Descriptions

Field	Description
Track	Object number that is being tracked.
Interface Ethernet1/0 line-protocol	Interface type, interface number, and object that is being tracked.
Line protocol is Down (carrier-delay)	State of the interface with the carrier-delay parameter taken into consideration.
last change	Time (in *hh:mm:ss*) since the state of a tracked object last changed.

Table 314 describes the significant fields shown in the displays.

Table 314 show track brief Field Descriptions

Field	Description
Track	Object number that is being tracked.
Object	Definition of stub object.
Parameter	Tracking parameters.
Value	State value of the object, displayed as Up or Down.
last change	Time (in *hh:mm:ss*) since the state of a tracked object last changed.

Related Commands

Command	Description
track interface	Configures an interface to be tracked and enters tracking configuration mode.
track ip route	Tracks the state of an IP route and enters tracking configuration mode.

show tunnel 6rd

To display IPv6 rapid deployment (6RD) information about a tunnel, use the **show tunnel 6rd** command in privileged EXEC mode.

show tunnel 6rd [*tunnel-interface interface-number*]

Syntax Description

tunnel-interface(interface-number	(Optional) Specifies a tunnel interface and number.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T.

Usage Guidelines

The **show tunnel 6rd** command displays 6RD-related information on a tunnel. If an interface is not specified, information about all the 6RD tunnels on the router is displayed.

Examples

The following is sample output from the show tunnel 6rd command:

```
Router# show tunnel 6rd tunnel 1

show tunnel 6rd tunnel 1
Interface Tunnel1:
  Tunnel Source: 10.1.2.1
  6RD: Operational, V6 Prefix: 2001:B000::/32
       V4 Prefix, Length: 16, Value: 10.1.0.0
       V4 Suffix, Length: 8, Value: 0.0.0.1
  General Prefix: 2001:B000:200::/40
```

Table 273 describes the significant fields shown in the display.

Table 315 show tunnel 6rd Field Descriptions

Field	Description
Interface Tunnel1:	The specified tunnel interface and number.
Tunnel Source: 10.1.2.1	The source address for the tunnel interface.
6RD: Operational	6RD is enabled on the router.
V6 Prefix: 2001:B000::/32	The common IPv6 prefix on IPv6 6RD tunnels.

Table 315 show tunnel 6rd Field Descriptions (continued)

Field	Description
V4 Common Prefix Length: 16, Value: 10.1.0.0	The prefix length and value of the IPv4 transport address common to all the 6RD routers in a domain.
V4 Common Suffix Length: 8, Value: 0.0.0.1	The suffix length and value of the IPv4 transport address common to all the 6RD routers in a domain.

Related Commands

Command	Description
tunnel 6rd prefix	Specifies the common IPv6 prefix on IPv6 6RD tunnels.
tunnel mode ipv6ip	Configures a static IPv6 tunnel interface.
tunnel source	Sets the source address for a tunnel interface.

show tunnel 6rd destination

To translate an IPv6 rapid deployment (6RD) prefix to the corresponding IPv4 destination, use the **show tunnel 6rd destination** command in privileged EXEC mode.

show tunnel 6rd destination *ipv6-prefix tunnel-interface interface-number*

Syntax Description

ipv6-prefix	The IPv6 network assigned to the general prefix.
tunnel-interface interface-number	Specifies a tunnel interface and number.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T.

Usage Guidelines

The **show tunnel 6rd destination** command is used to translate a 6RD prefix to the corresponding IPv4 destination. The IPv4 destination address is displayed in the command output.

Examples

The following is sample output from the **show tunnel 6rd destination** command:

```
Router# show tunnel 6rd destination 2001:B000:300:: tunnel 1

Interface: Tunnel1
6RD Prefix: 2001:B000:300::
Destination: 10.1.3.1.
```

Table 316 show tunnel 6rd destination Field Descriptions

Field	Description
Interface Tunnel1:	The specified tunnel interface and number.
6RD Prefix	The specified 6RD IPv6 prefix.
Destination: 10.1.3.1	The corresponding IPv4 destination.

Related Commands

Command	Description
tunnel 6rd prefix	Specifies the common IPv6 prefix on IPv6 6RD tunnels.
tunnel mode ipv6ip	Configures a static IPv6 tunnel interface.
tunnel source	Sets the source address for a tunnel interface.

show voip rtp connections

To display Real-Time Transport Protocol (RTP) named event packets, use the **show voip rtp connections** command in privileged EXEC mode.

show voip rtp connections [**detail**]

Syntax Description

detail	(Optional) Displays the called-party and calling-party numbers associated with a call.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0	This command was introduced.
12.3(7)T	The **detail** keyword was added.
12.3(14)T	This command was implemented on the Cisco 2800 series and Cisco 3800 series.
12.4(2)T	This command was integrated into Cisco IOS Release 12.4(2)T.
12.4(22)T	Command output was updated to show IPv6 information.

Usage Guidelines

This command displays information about RTP named event packets, such as caller ID number, IP address, and port for both the local and remote endpoints. The output from this command provides an overview of all the connections in the system, and this information can be used to narrow the criteria for debugging. The **debug voip rtp** command floods the console with voice packet information. You can use the **show voip rtp connections** command to get caller ID, remote IP address, or remote port identifiers that you can use to limit the output from the **debug voip rtp** command.

The **detail** keyword allows you to identify the phone or phones that have connected two RTP call legs to create VoIP-to-VoIP or VoIP-to-POTS hairpins. If the **detail** keyword is omitted, the output does not display calls that are connected by hairpin call routing.

Examples

Table 317 describes the significant fields shown in the examples. Each line of output under "VoIP RTP active connections" shows information for one call leg. A phone call normally consists of two call legs, one connected to the calling party and one connected to the called party. The router joins (or bridges) the two call legs to make a call. The **show voip rtp connections** command shows the RTP information for H.323 and Session Initiation Protocol (SIP) calls only; it does not directly show the POTS call legs. The information for the IP phone can be seen using the **show ephone offhook** command.

The following sample output shows an incoming H.323 call that is being directed to an IP phone attached to a Cisco CallManager Express (CME) system.

```
Router# show voip rtp connections

VoIP RTP active connections :
No. CallId  dstCallId  LocalRTP RmtRTP LocalIP          RemoteIP
1   21      22         16996    18174  10.4.204.37      10.4.204.24
```

```
Found 1 active RTP connections
```

The following sample output shows the same call as in the previous example, but using the **detail** keyword with the command. The sample output shows the called number (1509) and calling number (8108) on both call legs (21 and 22); the called and calling numbers are the same on both legs for a simple A-to-B call. Leg 21 is the H.323 segment of the and leg 22 is the POTS segment that goes to the IP phone.

```
Router# show voip rtp connections detail

VoIP RTP active connections :
No. CallId  dstCallId  LocalRTP RmtRTP LocalIP          RemoteIP
1   21      22         16996    18174  10.4.204.37      10.4.204.24
  callId 21 (dir=1):called=1509 calling=8108 redirect=
     dest callId 22:called=1509 calling=8108 redirect=
   1 context 64FB3358 xmitFunc 6032E8B4
Found 1 active RTP connections
```

The following example shows the call from the previous example being transferred by extension 1509 to extension 1514. Notice that the dstCallId changed from 22 to 24, but the original call leg (21) for the transferred party is still present. This implies that H.450.2 capability was disabled for this particular call, because if H.450.2 was being used for the transfer, the transfer would have caused the incoming H.323 call leg to be replaced with a new call.

```
Router# show voip rtp connections

VoIP RTP active connections :
No. CallId  dstCallId  LocalRTP RmtRTP LocalIP         RemoteIP
1   21      24         16996    18174  10.4.204.37      10.4.204.24
Found 1 active RTP connections
```

The following example shows the detailed output for the same transfer as shown in the previous example. The original incoming call leg is still present (21) and still has the original called and calling numbers. The transferred call leg (24) shows 1509 (the transferring party) as the calling party and 1514 (the transfer destination) as the called party.

```
Router# show voip rtp connections detail

VoIP RTP active connections :
No. CallId  dstCallId  LocalRTP RmtRTP LocalIP         RemoteIP
1   21      24         16996    18174  10.4.204.37      10.4.204.24
  callId 21 (dir=1):called=1509 calling=8108 redirect=
     dest callId 24:called=1514 calling=1509 redirect=
   1 context 6466E810 xmitFunc 6032E8B4
Found 1 active RTP connections
```

The following sample output shows a cross-linked call with two H.323 call legs. The first line of output shows that the CallID for the first call leg is 7 and that this call leg is associated with another call leg that has a destination CallId of 8. The next line shows that the CallID for the leg is 8 and that it is associated with another call leg that has a destination CallId of 7. This cross-linkage between CallIds 7 and 8 shows that the first call leg is related to the second call leg (and vice versa). From this you can infer that the two call legs are actually part of the same phone call.

In an active system you can expect many lines of output that you would have to sort through to see which ones have this cross-linkage relationship. The lines showing two related call legs are not necessarily listed in adjacent order.

```
Router# show voip rtp connections

VoIP RTP active connections :
No. CallId   dstCallId          LocalRTP     RmtRTP         LocalIP        RemoteIP
1        7           8             16586      22346      172.27.82.2      172.29.82.2
2        8           7             17010      16590      172.27.82.2      192.168.1.29
```

```
Found 2 active RTP connections
```

The following example shows RTP information with IPv6 local and remote addresses:

```
Router# show voip rtp connections

VoIP RTP active connections :
No.  CallId   dstCallId  LocalRTP  RmtRTP   LocalIP                              RemoteIP
1     11      9          17424     18282    2001:DB8:C18:1:218:FEFF:FE71:2AB6
2001:DB8:C18:1:218:FEFF:FE71:2AB6
2     12      10         18282     17424    2001:DB8:C18:1:218:FEFF:FE71:2AB6
2001:DB8:C18:1:218:FEFF:FE71:2AB6

Found 2 active RTP connections
```

Table 317 show voip rtp connections Field Descriptions

Field	Description
No.	Identifier of an RTP connection in this output.
CallId	Internal call identifier of a telephony call leg (RTP connection).
dstCallId	Internal call identifier of a VoIP call leg.
LocalRTP	RTP port of the media stream for the local entity.
RmtRTP	RTP port of the media stream for the remote entity.
LocalIP	IPv4 or IPv6 address of the media stream for the local entity.
RemoteIP	IPv4 or IPv6 address of the media stream for the remote entity.
dir	0 indicates an outgoing call. 1 indicates an incoming call.
called	Extension that received the call.
calling	Extension that made the call.
redirect	Original called number if the incoming call was forwarded.
context	Internal memory address for the control block associated with the call.
xmitFunc	Internal memory address for the transmit function to which incoming RTP packets (on the H.323 and SIP side) are sent; the address for the function that delivers the packets to the ephone.

Related Commands

Command	Description
debug voip rtp	Enables debugging for RTP named event packets.
show ephone offhook	Displays information and packet counts for phones that are currently off hook.

show vpdn session

To display session information about active Layer 2 sessions for a virtual private dialup network (VPDN), use the **show vpdn session** command in privileged EXEC mode.

show vpdn session [**l2f** | **l2tp** | **pptp**] [**all** | **packets** [**ipv6**] | **sequence** | **state** [*filter*]]

Syntax Description

l2f	(Optional) Displays information about Layer 2 Forwarding (L2F) calls only.
l2tp	(Optional) Displays information about Layer 2 Tunnel Protocol (L2TP) calls only.
pptp	(Optional) Displays information about Point-to-Point Tunnel Protocol (PPTP) calls only.
all	(Optional) Displays extensive reports about active sessions.
packets	(Optional) Displays information about packet and byte counts for sessions.
ipv6	(Optional) Displays IPv6 packet and byte-count statistics.
sequence	(Optional) Displays sequence information for sessions.
state	(Optional) Displays state information for sessions.
filter	(Optional) One of the filter parameters defined in Table 318.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.2	This command was introduced.
12.1(1)T	This command was enhanced to display Point-to-Point Protocol over Ethernet (PPPoE) session information. The **packets** and **all** keywords were added.
12.1(2)T	This command was enhanced to display PPPoE session information on actual Ethernet interfaces.
12.2(13)T	Reports from this command were enhanced with a unique identifier that can be used to correlate a particular session with the session information retrieved from other **show** commands or **debug** command traces.
12.3(2)T	The **l2f**, **l2tp**, and **pptp** keywords were added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.4(11)T	The **l2f** keyword was removed.
Cisco IOS XE Release 2.5	This command was implemented on Cisco ASR 1000 series routers.
Cisco IOS XE Release 2.6	The **ipv6** keyword was added. The **show vpdn session** command with the **all** and **l2tp all** keywords was modified to display IPv6 counter information.

Usage Guidelines

Use the **show vpdn session** command to display information about all active sessions using L2TP, L2F, and PPTP.

The output of the **show vpdn session** command displays PPPoE session information as well. PPPoE is supported on ATM permanent virtual connections (PVCs) compliant with RFC 1483 only. PPPoE is not supported on Frame Relay and any other LAN interfaces such as FDDI and Token Ring.

Reports and options for this command depend upon the configuration in which it is used. Use the command-line question mark (?) help function to display options available with the **show vpdn session** command.

Table 318 defines the filter parameters available to refine the output of the **show vpdn session** command. You may use any one of the filter parameters in place of the *filter* argument.

Table 318 Filter Parameters for the show vpdn session Command

Syntax	Description
interface serial *number*	Filters the output to display only information for sessions associated with the specified serial interface. • *number*—The serial interface number.
interface virtual-template *number*	Filters the output to display only information for sessions associated with the specified virtual template. • *number*—The virtual template number.
tunnel id *tunnel-id session-id*	Filters the output to display only information for sessions associated with the specified tunnel ID and session ID. • *tunnel-id*—The local tunnel ID. Valid values range from 1 to 65535. • *session-id*—The local session ID. Valid values range from 1 to 65535.
tunnel remote-name *remote-name local-name*	Filters the output to display only information for sessions associated with the tunnel with the specified names. • *remote-name*—The remote tunnel name. • *local-name*—The local tunnel name.
username *username*	Filters the output to display only information for sessions associated with the specified username. • *username*—The username.

The **show vpdn session** command provides reports on call activity for all active sessions. The following output is from a device carrying active L2TP, L2F, and PPPoE sessions:

```
Router# show vpdn session

L2TP Session Information Total tunnels 1 sessions 4

LocID RemID TunID Intf          Username             State    Last Chg Uniq ID
4     691   13695 Se0/0         nobody2@cisco.com        est    00:06:00  4
5     692   13695 SSS Circuit   nobody1@cisco.com        est    00:01:43  8
6     693   13695 SSS Circuit   nobody1@cisco.com        est    00:01:43  9
3     690   13695 SSS Circuit   nobody3@cisco.com        est    2d21h     3

L2F Session Information Total tunnels 1 sessions 2

 CLID   MID    Username                  Intf          State   Uniq ID
 1      2      nobody@cisco.com             SSS Circuit   open    10
 1      3      nobody@cisco.com             SSS Circuit   open    11
```

```
%No active PPTP tunnels

PPPoE Session Information Total tunnels 1 sessions 7

PPPoE Session Information
UID    SID    RemMAC         OIntf          Intf      Session
              LocMAC                        VASt      state
3      1      0030.949b.b4a0 Fa2/0          N/A       CNCT_FWDED
              0010.7b90.0840
6      2      0030.949b.b4a0 Fa2/0          Vi1.1     CNCT_PTA
              0010.7b90.0840                UP
7      3      0030.949b.b4a0 Fa2/0          Vi1.2     CNCT_PTA
              0010.7b90.0840                UP
8      4      0030.949b.b4a0 Fa2/0          N/A       CNCT_FWDED
              0010.7b90.0840
9      5      0030.949b.b4a0 Fa2/0          N/A       CNCT_FWDED
              0010.7b90.0840
10     6      0030.949b.b4a0 Fa2/0          N/A       CNCT_FWDED
              0010.7b90.0840
11     7      0030.949b.b4a0 Fa2/0          N/A       CNCT_FWDED
              0010.7b90.0840
```

Table 319 describes the significant fields shown in the **show vpdn session** display.

Table 319 show vpdn session Field Descriptions

Field	Description
LocID	Local identifier.
RemID	Remote identifier.
TunID	Tunnel identifier.
Intf	Interface associated with the session.
Username	User domain name.
State	Status for the individual user in the tunnel; can be one of the following states: • est • opening • open • closing • closed • waiting_for_tunnel The waiting_for_tunnel state means that the user connection is waiting until the main tunnel can be brought up before it moves to the opening state.
Last Chg	Time interval (in hh:mm:ss) since the last change occurred.
Uniq ID	The unique identifier used to correlate this particular session with the sessions retrieved from other **show** commands or **debug** command traces.
CLID	A number uniquely identifying the session.
MID	A number uniquely identifying this user in this tunnel.
UID	PPPoE user ID.

Table 319 show vpdn session Field Descriptions (continued)

Field	Description
SID	PPPoE session ID.
RemMAC	Remote MAC address of the host.
LocMAC	Local MAC address of the router. It is the default MAC address of the router.
OIntf	Outgoing interface.
Intf VASt	Virtual access interface number and state.
Session state	PPPoE session state.

The **show vpdn session packets** command provides reports on call activity for all the currently active sessions. The following output is from a device carrying an active PPPoE session:

```
Router# show vpdn session packets

%No active L2TP tunnels
%No active L2F tunnels

PPPoE Session Information Total tunnels 1 sessions 1
PPPoE Session Information
SID     Pkts-In         Pkts-Out        Bytes-In        Bytes-Out
1       202333          202337          2832652         2832716
```

Table 320 describes the significant fields shown in the **show vpdn session packets** command display.

Table 320 show vpdn session packets Field Descriptions

Field	Description
SID	Session ID for the PPPoE session.
Pkts-In	Number of packets coming into this session.
Pkts-Out	Number of packets going out of this session.
Bytes-In	Number of bytes coming into this session.
Bytes-Out	Number of bytes going out of this session.

The **show vpdn session all** command provides extensive reports on call activity for all the currently active sessions. The following output is from a device carrying active L2TP, L2F, and PPPoE sessions:

```
Router# show vpdn session all

L2TP Session Information Total tunnels 1 sessions 4

Session id 5 is up, tunnel id 13695
Call serial number is 3355500002
Remote tunnel name is User03
  Internet address is 10.0.0.63
  Session state is established, time since change 00:03:53
    52 Packets sent, 52 received
    2080 Bytes sent, 1316 received
  Last clearing of "show vpdn" counters never
  Session MTU is 1464 bytes
  Session username is nobody@cisco.com
    Interface
```

```
    Remote session id is 692, remote tunnel id 58582
  UDP checksums are disabled
  SSS switching enabled
  No FS cached header information available
  Sequencing is off
  Unique ID is 8

Session id 6 is up, tunnel id 13695
Call serial number is 3355500003
Remote tunnel name is User03
  Internet address is 10.0.0.63
  Session state is established, time since change 00:04:22
    52 Packets sent, 52 received
    2080 Bytes sent, 1316 received
  Last clearing of "show vpdn" counters never
  Session MTU is 1464 bytes
  Session username is nobody@cisco.com
    Interface
    Remote session id is 693, remote tunnel id 58582
  UDP checksums are disabled
  SSS switching enabled
  No FS cached header information available
  Sequencing is off
  Unique ID is 9

Session id 3 is up, tunnel id 13695
Call serial number is 3355500000
Remote tunnel name is User03
  Internet address is 10.0.0.63
  Session state is established, time since change 2d21h
    48693 Packets sent, 48692 received
    1947720 Bytes sent, 1314568 received
  Last clearing of "show vpdn" counters never
  Session MTU is 1464 bytes
  Session username is nobody2@cisco.com
    Interface
    Remote session id is 690, remote tunnel id 58582
  UDP checksums are disabled
  SSS switching enabled
  No FS cached header information available
  Sequencing is off
  Unique ID is 3

Session id 4 is up, tunnel id 13695
Call serial number is 3355500001
Remote tunnel name is User03
  Internet address is 10.0.0.63
  Session state is established, time since change 00:08:40
    109 Packets sent, 3 received
    1756 Bytes sent, 54 received
  Last clearing of "show vpdn" counters never
  Session MTU is 1464 bytes
  Session username is nobody@cisco.com
    Interface Se0/0
    Remote session id is 691, remote tunnel id 58582
  UDP checksums are disabled
  IDB switching enabled
  FS cached header information:
    encap size = 36 bytes
    4500001C BDDC0000 FF11E977 0A00003E
    0A00003F 06A506A5 00080000 0202E4D6
    02B30000
  Sequencing is off
  Unique ID is 4
```

```
L2F Session Information Total tunnels 1 sessions 2
MID: 2
User:  nobody@cisco.com
Interface:
State:  open
Packets out: 53
Bytes out: 2264
Packets in: 51
Bytes in: 1274
Unique ID: 10

  Last clearing of "show vpdn" counters never
MID: 3
User:  nobody@cisco.com
Interface:
State:  open
Packets out: 53
Bytes out: 2264
Packets in: 51
Bytes in: 1274
Unique ID: 11

Last clearing of "show vpdn" counters never

%No active PPTP tunnels

PPPoE Session Information Total tunnels 1 sessions 7

PPPoE Session Information
SID     Pkts-In         Pkts-Out        Bytes-In        Bytes-Out
1       48696           48696           681765          1314657
2       71              73              1019            1043
3       71              73              1019            1043
4       61              62              879             1567
5       61              62              879             1567
6       55              55              791             1363
7       55              55              795             1363
```

The significant fields shown in the **show vpdn session all** command display are similar to those defined in Table 319 and Table 320.

Related Commands

Command	Description
show sss session	Displays Subscriber Service Switch session status.
show vpdn	Displays basic information about all active VPDN tunnels.
show vpdn domain	Displays all VPDN domains and DNIS groups configured on the NAS.
show vpdn group	Displays a summary of the relationships among VPDN groups and customer/VPDN profiles, or summarizes the configuration of a VPDN group including DNIS/domain, load sharing information, and current session information.
show vpdn history failure	Displays the content of the failure history table.
show vpdn multilink	Displays the multilink sessions authorized for all VPDN groups.
show vpdn redirect	Displays statistics for L2TP redirects and forwards.
show vpdn tunnel	Displays information about active Layer 2 tunnels for a VPDN.

show vpdn tunnel

To display information about active Layer 2 tunnels for a virtual private dialup network (VPDN), use the **show vpdn tunnel** command in privileged EXEC mode.

show vpdn tunnel [**l2f** | **l2tp** | **pptp**] [**all** [*filter*] | **packets** [**ipv6**] [*filter*] | **state** [*filter*] | **summary** [*filter*] | **transport** [*filter*]]

Syntax Description

l2f	(Optional) Specifies that only information about Layer 2 Forwarding (L2F) tunnels will be displayed.
l2tp	(Optional) Specifies that only information about Layer 2 Tunnel Protocol (L2TP) tunnels will be displayed.
pptp	(Optional) Specifies that only information about Point-to-Point Tunnel Protocol (PPTP) tunnels will be displayed.
all	(Optional) Displays summary information about all active tunnels.
filter	(Optional) One of the filter parameters defined in Table 321.
packets	(Optional) Displays packet numbers and packet byte information.
ipv6	(Optional) Displays IPv6 packet and byte-count statistics.
state	(Optional) Displays state information for a tunnel.
summary	(Optional) Displays a summary of tunnel information.
transport	(Optional) Displays tunnel transport information.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.1(1)T	The **packet**s and **all** keywords were added.
12.3(2)T	The **l2f**, **l2tp**, and **pptp** keywords were added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and support was added for L2TP congestion avoidance statistics.
12.4(11)T	The **l2f** keyword was removed.
12.2(33)SB	This command's output was modified and implemented on the Cisco 10000 series router for the PRE3 and PRE4 as described in the Usage Guidelines.
Cisco IOS XE Release 2.6	The **ipv6** keyword was added. The **show vpdn tunnel** command with the **all** and **l2tp all** keywords was modified to display IPv6 counter information.

Usage Guidelines

Use the **show vpdn tunnel** command to display detailed information about L2TP, L2F, and PPTP VPDN tunnels.

Table 321 defines the filter parameters available to refine the output of the **show vpdn tunnel** command. You may use any one of the filter parameters in place of the *filter* argument.

Table 321 Filter Parameters for the show vpdn tunnel Command

Syntax	Description
id *local-id*	Filters the output to display only information for the tunnel with the specified local ID. • *local-id*—The local tunnel ID number. Valid values range from 1 to 65535.
local-name *local-name remote-name*	Filters the output to display only information for the tunnel associated with the specified names. • *local-name*—The local tunnel name. • *remote-name*—The remote tunnel name.
remote-name *remote-name local-name*	Filters the output to display only information for the tunnel associated with the specified names. • *remote-name*—The remote tunnel name. • *local-name*—The local tunnel name.

Cisco 10000 Series Router Usage Guidelines

In Cisco IOS Release 12.2(33)SB, the **show vpdn tunnel summary** command no longer displays the active PPPoE sessions. Instead, use the **show pppoe sessions** command to display the active sessions.

In Cisco IOS Release 12.2(31)SB, the **show vpdn tunnel summary** command does display the active PPPoE sessions.

Examples

The following is sample output from the **show vpdn tunnel** command for L2F and L2TP sessions:

```
Router# show vpdn tunnel

L2TP Tunnel Information (Total tunnels=1 sessions=1)
LocID RemID Remote Name   State  Remote Address  Port  Sessions
2     10    router1       est    172.21.9.13     1701  1

L2F Tunnel
 NAS CLID HGW CLID NAS Name        HGW Name        State
 9         1        nas1           HGW1            open
                    172.21.9.4      172.21.9.232

%No active PPTP tunnels
```

Table 322 describes the significant fields shown in the display.

Table 322 show vpdn tunnel Field Descriptions

Field	Description
LocID	Local tunnel identifier.
RemID	Remote tunnel identifier.
Remote Name	Hostname of the remote peer.

Table 322 show vpdn tunnel Field Descriptions (continued)

Field	Description
State	Status for the individual user in the tunnel; can be one of the following states: • est • opening • open • closing • closed • waiting_for_tunnel The waiting_for_tunnel state means that the user connection is waiting until the main tunnel can be brought up before it moves to the opening state.
Remote address	IP address of the remote peer.
Port	Port ID.
Sessions	Number of sessions using the tunnel.
NAS CLID	A number uniquely identifying the VPDN tunnel on the network access server (NAS).
HGW CLID	A number uniquely identifying the VPDN tunnel on the gateway.
NAS Name	Hostname and IP address of the NAS.
HGW Name	Hostname and IP address of the home gateway.

The following example shows L2TP tunnel activity, including information about the L2TP congestion avoidance:

```
Router# show vpdn tunnel l2tp all

L2TP Tunnel Information Total tunnels 1 sessions 1

Tunnel id 30597 is up, remote id is 45078, 1 active sessions
  Tunnel state is established, time since change 00:08:27
  Tunnel transport is UDP (17)
  Remote tunnel name is LAC1
    Internet Address 172.18.184.230, port 1701
  Local tunnel name is LNS1
    Internet Address 172.18.184.231, port 1701
  Tunnel domain unknown
  VPDN group for tunnel is 1
  L2TP class for tunnel is
  4 packets sent, 3 received
  194 bytes sent, 42 received
  Last clearing of "show vpdn" counters never
  Control Ns 2, Nr 4
  Local RWS 1024 (default), Remote RWS 256
  In Use Remote RWS 15
  Control channel Congestion Control is enabled
    Congestion Window size, Cwnd 3
    Slow Start threshold, Ssthresh 256
    Mode of operation is Slow Start
  Tunnel PMTU checking disabled
  Retransmission time 1, max 2 seconds
  Unsent queuesize 0, max 0
  Resend queuesize 0, max 1
```

```
Total resends 0, ZLB ACKs sent 2
Current nosession queue check 0 of 5
Retransmit time distribution: 0 0 0 0 0 0 0 0 0
Sessions disconnected due to lack of resources 0
Control message authentication is disabled
```

Table 323 describes the significant fields shown in the display.

Table 323 show vpdn tunnel all Field Descriptions

Field	Description
Local RWS	Size of the locally configured receive window.
Remote RWS	Size of the receive window advertised by the remote peer.
In Use RWS	Actual size of the receive window, if that value differs from the value advertised by the remote peer.
Congestion Window size, Cwnd 3	Current size of the congestion window (Cwnd).
Slow Start threshold, Ssthresh 500	Current value of the slow start threshold (Ssthresh).
Mode of operation is...	Indicates if the router is operating in Slow Start or Congestion Avoidance mode.

Related Commands

Command	Description
show vpdn	Displays basic information about all active VPDN tunnels.
show vpdn domain	Displays all VPDN domains and DNIS groups configured on the NAS.
show vpdn group	Displays a summary of the relationships among VPDN groups and customer/VPDN profiles, or summarizes the configuration of a VPDN group including DNIS/domain, load sharing information, and current session information.
show vpdn history failure	Displays the content of the failure history table.
show vpdn multilink	Displays the multilink sessions authorized for all VPDN groups.
show vpdn redirect	Displays statistics for L2TP redirects and forwards.
show vpdn session	Displays session information about active Layer 2 sessions for a VPDN.

show vrf

To display the defined Virtual Private Network (VPN) routing and forwarding (VRF) instances, use the **show vrf** command in user EXEC or privileged EXEC mode.

show vrf [**ipv4** | **ipv6**] [**interface** | **brief** | **detail** | **id** | **select** | **lock**] [*vrf-name*]

Syntax Description

ipv4	(Optional) Displays IPv4 address family-type VRF instances.
ipv6	(Optional) Displays IPv6 address family-type VRF instances.
interface	(Optional) Displays the interface associated with the specified VRF instances.
brief	(Optional) Displays brief information about the specified VRF instances.
detail	(Optional) Displays detailed information about the specified VRF instances.
id	(Optional) Displays VPN-ID information for the specified VRF instances.
select	(Optional) Displays selection information for the specified VRF instances.
lock	(Optional) Displays VPN lock information for the specified VRF instances.
vrf-name	(Optional) Name assigned to a VRF.

Command Default

If you do not specify any arguments or keywords, the command displays concise information about all configured VRFs.

Command Modes

User EXEC (>)
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.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. When backup paths have been created either through the Prefix Independent Convergence or Best External feature, the output of the **show vrf detail** command displays the following line: `Prefix protection with additional path enabled`
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.

Usage Guidelines

Use the **show vrf** command to display information about specified VRF instances or all VRF instances. Specify no arguments or keywords to display information on all VRF instances.

Examples

The following sample output from the **show vrf** command displays brief information about all configured VRF instances:

```
Router# show vrf

  Name                              Default RD          Protocols   Interfaces
  N1                                100:0               ipv4,ipv6
  V1                                1:1                 ipv4        Lo1
  V2                                2:2                 ipv4,ipv6   Et0/1.1
                                                                    Et0/1.2
                                                                    Et0/1.3
  V3                                3:3                 ipv4        Lo3
                                                                    Et0/1.4
```

Table 324 describes the significant fields shown in the display.

Table 324 show vrf Field Descriptions

Field	Description
Name	Name of the VRF instance.
Default RD	The default route distinguisher (RD) for the specified VRF instances.
Protocols	The address family protocol type for the specified VRF instance.
Interfaces	The network interface associated with the VRF instance.

The following sample output from the **show vrf** command with the **detail** keyword displays information for a VRF named cisco:.

```
Router# show vrf detail

VRF cisco1; default RD 100:1; default VPNID <not set>
  Interfaces:
    Ethernet0/0                 Loopback10
Address family ipv4 (Table ID = 0x1):
  Connected addresses are not in global routing table
  Export VPN route-target communities
    RT:100:1
  Import VPN route-target communities
    RT:100:1
  No import route-map
  No export route-map
  VRF label distribution protocol: not configured
Address family ipv6 (Table ID = 0xE000001):
  Connected addresses are not in global routing table
  Export VPN route-target communities
    RT:100:1
  Import VPN route-target communities
    RT:100:1
  No import route-map
  No export route-map
  VRF label distribution protocol: not configured
```

Table 325 describes the significant fields shown in the display.

Table 325 show vrf detail Field Descriptions

Field	Description
default RD 100:1	The RD given to this VRF.
Interfaces:	Interfaces to which the VRF is attached.
Export VPN route-target communities RT:100:1	Route-target VPN extended communities to be exported.
Import VPN route-target communities RT:100:1	Route-target VPN extended communities to be imported.

The following example displays output from the **show vrf detail** command when backup paths have been created either through the Prefix Independent Convergence or Best External feature. The output of the **show vrf detail** command displays the following line:

```
Prefix protection with additional path enabled
```

```
Router# show vrf detail

VRF vpn1 (VRF Id = 1); default RD 1:1; default VPNID <not set>
  Interfaces:
    Et1/1
Address family ipv4 (Table ID = 1 (0x1)):
  Export VPN route-target communities
    RT:1:1
  Import VPN route-target communities
    RT:1:1
  No import route-map
  No export route-map
  VRF label distribution protocol: not configured
  VRF label allocation mode: per-prefix
  Prefix protection with additional path enabled
Address family ipv6 not active.
```

The following sample output from the **show vrf lock** command displays VPN lock information:

```
Router# show vrf lock

VRF Name: Mgmt-intf; VRF id = 4085 (0xFF5)
VRF lock count: 3
         Lock user: RTMGR, lock user ID: 2, lock count per user: 1
         Caller PC tracebacks:
         Trace backs: :10000000+44DAEB4 :10000000+21E83AC :10000000+45A9F04 :108
         Lock user: CEF, lock user ID: 4, lock count per user: 1
         Caller PC tracebacks:
         Trace backs: :10000000+44DAEB4 :10000000+21E83AC :10000000+45A9F04 :10C
         Lock user: VRFMGR, lock user ID: 1, lock count per user: 1
         Caller PC tracebacks:
         Trace backs: :10000000+44DAEB4 :10000000+21E83AC :10000000+21EAD18 :10C
VRF Name: vpn1; VRF id = 1 (0x1)
VRF lock count: 3
         Lock user: RTMGR, lock user ID: 2, lock count per user: 1
         Caller PC tracebacks:
         Trace backs: :10000000+44DAEB4 :10000000+21E83AC :10000000+45A9F04 :10C
         Lock user: CEF, lock user ID: 4, lock count per user: 1
         Caller PC tracebacks:
         Trace backs: :10000000+44DAEB4 :10000000+21E83AC :10000000+45A9F04 :100
```

```
Lock user: VRFMGR, lock user ID: 1, lock count per user: 1
Caller PC tracebacks:
Trace backs: :10000000+44DAEB4 :10000000+21E83AC :10000000+21EAD18 :10C
```

Related Commands

Command	Description
vrf definition	Configures a VRF routing table instance and enters VRF configuration mode.
vrf forwarding	Associates a VRF instance with an interface or subinterface.

shutdown (gateway)

To shut down all VoIP call service on a gateway, use the **shutdown** command in voice service configuration mode. To enable VoIP call service, use the **no** form of this command.

shutdown [**forced**]

no shutdown

Syntax Description

forced	(Optional) Forces the gateway to immediately terminate all in-progress calls.

Command Default

Call service is enabled

Command Modes

Voice service configuration (config-voi-serv)

Command History

Release	Modification
12.3(1)	This command was introduced.

Examples

The following example shows VoIP call service being shut down on a Cisco gateway:

```
voice service voip
shutdown
```

The following example shows VoIP call service being enabled on a Cisco gateway:

```
voice service voip
no shutdown
```

Related Commands

Command	Description
shutdown (gatekeeper)	Disables the gatekeeper.

single-connection

To enable all TACACS packets to be sent to the same server using a single TCP connection, use the **single-connection** command in TACACS+ server configuration mode. To disable this feature, use the **no** form of this command.

single-connection

no single-connection

Syntax Description

This command has no arguments or keywords.

Command Default

TACACS packets are not sent on a single TCP connection.

Command Modes

TACACS+ server configuration (config-server-tacacs)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines

Use the **single-connection** command to multiplex all TACACS packets to the same server over a single TCP connection.

Examples

The following example shows how to multiplex all TACACS packets over a single TCP connection to the TACACS server:

```
Router (config)# tacacs server server1
Router(config-server-tacacs)# single-connection
```

Related Commands

Command	Description
tacacs server	Configures the TACACS+ server for IPv6 or IPv4 and enters config server tacacs mode.

sip address

To configure a Session Initiation Protocol (SIP) server IPv6 address to be returned in the SIP server's IPv6 address list option to clients, use the **sip address** command in DHCP for IPv6 pool configuration mode. To disable this feature, use the **no** form of this command.

sip address *ipv6-address*

no sip address *ipv6-address*

Syntax Description

ipv6-address	An IPv6 address. The *ipv6-address* argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

Command Default

No default behavior or values

Command Modes

DHCP for IPv6 pool 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 12.2(33)SRA.
Cisco IOS XE Release 2.5	This command was updated. It was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

For the Dynamic Host Configuration Protocol (DHCP) for IPv6 server to obtain prefixes from RADIUS servers, the user must also configure the authorization, authentication, and accounting (AAA) client and PPP on the router. For information on how to configure the AAA client and PPP, see the "Implementing ADSL and Deploying Dial Access for IPv6" module.

The **sip address** command configures a SIP server IPv6 address to be returned in the SIP server's IPv6 address list option to clients. To configure multiple SIP server addresses, issue this command multiple times. The new addresses will not overwrite old ones.

Examples

In the following example, the SIP server IPv6 address 2001:0db8::2 is configured to be returned in the SIP server's IPv6 address list option to clients:

```
sip address 2001:0DB8::2
```

Related Commands

Command	Description
prefix-delegation aaa	Specifies that prefixes are to be acquired from AAA servers.
sip domain-name	Configures an SIP server domain name to be returned in the SIP server's domain name list option to clients.

sip domain-name

To configure a Session Initiation Protocol (SIP) server domain name to be returned in the SIP server's domain name list option to clients, use the **sip domain-name** command in DHCP for IPv6 pool configuration mode. To disable this feature, use the **no** form of this command.

sip domain-name *domain-name*

no sip domain-name *domain-name*

Syntax Description

domain-name	A domain name for a DHCP for IPv6 client.

Command Default

No default behavior or values.

Command Modes

DHCP for IPv6 pool 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 12.2(33)SRA.
Cisco IOS XE Release 2.5	This command was updated. It was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

In order for the Dynamic Host Configuration Protocol (DHCP) for IPv6 server to obtain prefixes from RADIUS servers, the user must also configure the authorization, authentication, and accounting (AAA) client and PPP on the router. For information on how to configure the AAA client and PPP, see the "Implementing ADSL and Deploying Dial Access for IPv6" module.

The **sip domain-name** command configures a SIP server domain name to be returned in the SIP server's domain name list option to clients. To configure multiple SIP server domain names, issue this command multiple times. The new domain names will not overwrite old ones.

Examples

The following example configures the SIP server domain name sip1.cisco.com to be returned in the SIP server's domain name list option to clients:

```
sip domain-name sip1.cisco.com
```

Related Commands

Command	Description
prefix-delegation aaa	Specifies that prefixes are to be acquired from AAA servers.
sip address	Configures a SIP server IPv6 address to be returned in the SIP server's IPv6 address list option to clients.

sip-server

To configure a network address for the Session Initiation Protocol (SIP) server interface, use the **sip-server** command in SIP user-agent configuration mode. To remove a network address configured for SIP, use the **no** form of this command.

sip-server {**dns:**[*host-name*] | **ipv4:***ipv4-address* | **ipv6:**[*ipv6-address*][**:***port-num*]}

no sip-server

Syntax Description

dns:	Sets the global SIP server interface to a Domain Name System (DNS) hostname. If you do not specify a hostname, the default DNS defined by the **ip name-server** command is used.
host-name	(Optional) Valid DNS hostname in the following format: name.gateway.xyz.
ipv4:*ipv4-address*	Sets the global SIP server interface to an IPv4 address. A valid IPv4 address takes the following format: xxx.xxx.xxx.xxx.
ipv6:[*ipv6-address*]	Sets the global SIP server interface to an IPv6 address. You must enter brackets around the IPv6 address.
:*port-num*	(Optional) Port number for the SIP server.

Command Default

No network address is configured.

Command Modes

SIP user-agent configuration (conf-serv-sip)

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was implemented on the Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 was not included in this release.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T. This command was implemented on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850.
12.4(22)T	Support for IPv6 was added.

Usage Guidelines

If you use this command, you can also use the **session target sip-server** command on each dial peer instead of repeatedly entering the SIP server interface address for each dial peer. Configuring a SIP server as a session target is useful if a Cisco SIP proxy server (SPS) is present in the network. With an SPS, you can configure the SIP server option and have the interested dial peers use the SPS by default.

To reset this command to a null value, use the **default** command.

To configure an IPv6 address, the user must enter brackets [ ] around the IPv6 address.

Examples

The following example, beginning in global configuration mode, sets the global SIP server interface to the DNS hostname "3660-2.sip.com." If you also use the **session target sip server** command, you need not set the DNS hostname for each individual dial peer.

```
sip-ua
 sip-server dns:3660-2.sip.com

dial-peer voice 29 voip
 session target sip-server
```

The following example sets the global SIP server interface to an IPv4 address:

```
sip-ua
 sip-server ipv4:10.0.2.254
```

The following example sets the global SIP server interface to an IPv6 address. Note that brackets were entered around the IPv6 address:

```
sip-ua
 sip-server ipv6:[2001:0DB8:0:0:8:800:200C:417A]
```

Related Commands

Command	Description
default	Enables a default aggregation cache.
ip name-server	Specifies the address of one or more name servers to use for name and address resolution.
session target (VoIP dial peer)	Specifies a network-specific address for a dial peer.
session target sip-server	Instructs the dial peer session target to use the global SIP server.
sip-ua	Enters SIP user-agent configuration mode in order to configure the SIP user agent.

snmp-server community

To set up the community access string to permit access to the Simple Network Management Protocol (SNMP), use the **snmp-server community** command in global configuration mode. To remove the specified community string, use the **no** form of this command.

snmp-server community *string* [**view** *view-name*] [**ro** | **rw**] [**ipv6** *nacl*] [*access-list-number* | *extended-access-list-number* | *access-list-name*]

no snmp-server community *string*

Syntax Description

string	Community string that consists of 1 to 32 alphanumeric characters and functions much like a password, permitting access to SNMP. Blank spaces are not permitted in the community string. **Note** The @ symbol is used for delimiting the context information. Avoid using the @ symbol as part of the SNMP community string when configuring this command.
view	(Optional) Specifies a previously defined view. The view defines the objects available to the SNMP community.
view-name	(Optional) Name of a previously defined view.
ro	(Optional) Specifies read-only access. Authorized management stations can retrieve only MIB objects.
rw	(Optional) Specifies read-write access. Authorized management stations can both retrieve and modify MIB objects.
ipv6	(Optional) Specifies an IPv6 named access list.
nacl	(Optional) IPv6 named access list.
access-list-number	(Optional) Integer from 1 to 99 that specifies a standard access list of IP addresses or a string (not to exceed 64 characters) that is the name of a standard access list of IP addresses allowed access to the SNMP agent. Alternatively, an integer from 1300 to 1999 that specifies a list of IP addresses in the expanded range of standard access list numbers that are allowed to use the community string to gain access to the SNMP agent.

Command Default

An SNMP community string permits read-only access to all objects.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.0(14)ST	This command was integrated into Cisco IOS Release 12.0(14)ST.
12.0(17)S	This command was integrated into Cisco IOS Release 12.0(17)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.

Release	Modification
12.3(2)T	The access list values were enhanced to support the expanded range of standard access list values and to support named standard access lists.
12.0(27)S	The **ipv6** *nacl* keyword and argument pair was added to support assignment of IPv6 named access lists. This keyword and argument pair is not supported in Cisco IOS 12.2S releases.
12.3(14)T	The **ipv6** *nacl* keyword and argument pair was integrated into Cisco IOS Release 12.3(14)T to support assignment of IPv6 named access lists. This keyword and argument pair is not supported in Cisco IOS 12.2S releases.
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	This command was integrated into Cisco IOS Release 12.4(11)T.
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.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Aggregation Series Routers.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SRE	This command was modified. The automatic insertion of the **snmp-server community** command into the configuration, along with the community string specified in the **snmp-server host** command, is changed. The **snmp-server community** command has to be manually configured.
15.1(0)M	This command was modified. The automatic insertion of the **snmp-server community** command into the configuration, along with the community string specified in the **snmp-server host** command, is changed. The **snmp-server community** command has to be manually configured.

Usage Guidelines

The **no snmp-server** command disables all versions of SNMP (SNMPv1, SNMPv2C, SNMPv3).

The first **snmp-server** command that you enter enables all versions of SNMP.

To configure SNMP community strings for the MPLS LDP MIB, use the **snmp-server community** command on the host network management station (NMS).

Note In Cisco IOS Release 12.0(3) to 12.2(33)SRD, if a community string was not defined using the **snmp-server community** command prior to using the **snmp-server host** command, the default form of the **snmp-server community** command was automatically inserted into the configuration. The password (community string) used for this automatic configuration of the **snmp-server community** was same as specified in the **snmp-server host** command. However, in Cisco IOS Release 12.2(33)SRE and later releases, you have to manually configure the **snmp-server community** command.

The **snmp-server community** command can be used to specify only an IPv6 named access list, only an IPv4 access list, or both. For you to configure both IPv4 and IPv6 access lists, the IPv6 access list must appear first in the command statement.

Note The @ symbol is used as a delimiter between the community string and the context in which it is used. For example, specific VLAN information in BRIDGE-MIB may be polled using community@VLAN_ID (for example, public@100) where 100 is the VLAN number. Avoid using the @ symbol as part of the SNMP community string when configuring this command.

Examples

The following example shows how to set the read/write community string to newstring:

```
Router(config)# snmp-server community newstring rw
```

The following example shows how to allow read-only access for all objects to members of the standard named access list lmnop that specify the comaccess community string. No other SNMP managers have access to any objects.

```
Router(config)# snmp-server community comaccess ro lmnop
```

The following example shows how to assign the string comaccess to SNMP, allow read-only access, and specify that IP access list 4 can use the community string:

```
Router(config)# snmp-server community comaccess ro 4
```

The following example shows how to assign the string manager to SNMP and allow read-write access to the objects in the restricted view:

```
Router(config)# snmp-server community manager view restricted rw
```

The following example shows how to remove the community comaccess:

```
Router(config)# no snmp-server community comaccess
```

The following example shows how to disable all versions of SNMP:

```
Router(config)# no snmp-server
```

The following example shows how to configure an IPv6 access list named list1 and links an SNMP community string with this access list:

```
Router(config)# ipv6 access-list list1
Router(config-ipv6-acl)# permit ipv6 any any
Router(config-ipv6-acl)# exit
Router(config)# snmp-server community comaccess rw ipv6 list1
```

Related Commands

Command	Description
access-list	Configures the access list mechanism for filtering frames by protocol type or vendor code.
show snmp community	Displays SNMP community access strings.
snmp-server enable traps	Enables the router to send SNMP notification messages to a designated network management workstation.
snmp-server host	Specifies the targeted recipient of an SNMP notification operation.
snmp-server view	Creates or updates a view entry.

snmp-server engineID remote

To specify the Simple Network Management Protocol (SNMP) engine ID of a remote SNMP device, use the **snmp-server engineID remote** command in global configuration mode. To remove a specified SNMP engine ID from the configuration, use the **no** form of this command.

snmp-server engineID remote {*ipv4-ip-address* | *ipv6 address*}[**udp-port** *udp-port-number*] [**vrf** *vrf-name*] *engineid-string*

no snmp-server engineID remote {*ipv4-ip-address* | *ipv6 address*} [**udp-port** *udp-port-number*] [**vrf** *vrf-name*] *engineid-string*

Syntax Description

ipv4-ip-address | *ipv6-address*	IPv4 or IPv6 address of the device that contains the remote copy of SNMP.
udp-port	(Optional) Specifies a User Datagram Protocol (UDP) port of the host to use.
udp-port-number	(Optional) Socket number on the remote device that contains the remote copy of SNMP. The default is 161.
vrf	(Optional) Specifies an instance of a routing table.
vrf-name	(Optional) Name of the Virtual Private Network (VPN) routing and forwarding (VRF) table to use for storing data.
engineid-string	String of a maximum of 24 characters that identifies the engine ID.

Command Default

The default is UDP port 161.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2(2)T	The **vrf** keyword and *vrf-name* argument were added.
12.0(27)S	Support for configuring an IPv6 notification server was added.
12.3(14)T	Support for configuring an IPv6 notification server was added.
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 introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

Specifying the entire 24-character engine ID if it contains trailing zeros is not required. Specify only the portion of the engine ID up to where the trailing zeros start. For example, to configure an engine ID of 123400000000000000000000, specify the value 1234 as the *engineid-string* argument.

A remote engine ID is required when an SNMP version 3 inform is configured. The remote engine ID is used to compute the security digest for authenticating and encrypting packets sent to a user on the remote host.

Examples

The following example specifies the SNMP engine ID and configures the VRF name traps-vrf for SNMP communications with the remote device at 172.16.20.3:

```
Router(config)# snmp-server engineID remote 172.16.20.3 vrf traps-vrf
80000009030000B064EFE100
```

Related Commands

Command	Description
show snmp engineID	Displays the identification of the local SNMP engine and all remote engines that have been configured on the router.
snmp-server host	Specifies the recipient (SNMP manager) of an SNMP trap notification.

snmp-server group

To configure a new Simple Network Management Protocol (SNMP) group, use the **snmp-server group** command in global configuration mode. To remove a specified SNMP group, use the **no** form of this command.

snmp-server group *group-name* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**context** *context-name*] [**read** *read-view*] [**write** *write-view*] [**notify** *notify-view*] [**access** [**ipv6** *named-access-list*] [*acl-number* | *acl-name*]]

no snmp-server group *group-name* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**context** *context-name*]

Syntax Description

group-name	Name of the group.
v1	Specifies that the group is using the SNMPv1 security model. SNMPv1 is the least secure of the possible SNMP security models.
v2c	Specifies that the group is using the SNMPv2c security model. The SNMPv2c security model allows informs to be transmitted and supports 64-character strings.
v3	Specifies that the group is using the SNMPv3 security model. SMNPv3 is the most secure of the supported security models. It allows you to explicitly configure authentication characteristics.
auth	Specifies authentication of a packet without encrypting it.
noauth	Specifies no authentication of a packet.
priv	Specifies authentication of a packet with encryption.
context	(Optional) Specifies the SNMP context to associate with this SNMP group and its views.
context-name	(Optional) Context name.
read	(Optional) Specifies a read view for the SNMP group. This view enables you to view only the contents of the agent.
read-view	(Optional) String of a maximum of 64 characters that is the name of the view. The default is that the read-view is assumed to be every object belonging to the Internet object identifier (OID) space (1.3.6.1), unless the **read** option is used to override this state.
write	(Optional) Specifies a write view for the SNMP group. This view enables you to enter data and configure the contents of the agent.
write-view	(Optional) String of a maximum of 64 characters that is the name of the view. The default is that nothing is defined for the write view (that is, the null OID). You must configure write access.
notify	(Optional) Specifies a notify view for the SNMP group. This view enables you to specify a notify, inform, or trap.

notify-view	(Optional) String of a maximum of 64 characters that is the name of the view. By default, nothing is defined for the notify view (that is, the null OID) until the **snmp-server host** command is configured. If a view is specified in the **snmp-server group** command, any notifications in that view that are generated will be sent to all users associated with the group (provided a SNMP server host configuration exists for the user). Cisco recommends that you let the software autogenerate the notify view. See the "Configuring Notify Views" section in this document.
access	(Optional) Specifies a standard access control list (ACL) to associate with the group.
ipv6	(Optional) Specifies an IPv6 named access list. If both IPv6 and IPv4 access lists are indicated, the IPv6 named access list must appear first in the list.
named-access-list	(Optional) Name of the IPv6 access list.
acl-number	(Optional) The *acl-number* argument is an integer from 1 to 99 that identifies a previously configured standard access list.
acl-name	(Optional) The *acl-name* argument is a string of a maximum of 64 characters that is the name of a previously configured standard access list.

Command Default

No SNMP server groups are configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.(3)T	This command was introduced.
12.0(23)S	The **context** *context-name* keyword and argument pair was added.
12.3(2)T	The **context** *context-name* keyword and argument pair was integrated into Cisco IOS Release 12.3(2)T, and support for standard named access lists (acl-name) was added.
12.0(27)S	The **ipv6** *named-access-list* keyword and argument pair was added.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(14)T	The **ipv6** *named-access-list* keyword and argument pair was integrated into Cisco IOS Release 12.3(14)T.
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.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

When a community string is configured internally, two groups with the name public are autogenerated, one for the v1 security model and the other for the v2c security model. Similarly, deleting a community string will delete a v1 group with the name public and a v2c group with the name public.

No default values exist for authentication or privacy algorithms when you configure the **snmp-server group** command. Also, no default passwords exist. For information about specifying a Message Digest 5 (MD5) password, see the documentation of the **snmp-server user** command.

Configuring Notify Views

The *notify-view* option is available for two reasons:

- If a group has a notify view that is set using SNMP, you may need to change the notify view.
- The **snmp-server host** command may have been configured before the **snmp-server group** command. In this case, you must either reconfigure the **snmp-server host** command, or specify the appropriate notify view.

Specifying a notify view when configuring an SNMP group is not recommended, for the following reasons:

- The **snmp-server host** command autogenerates a notify view for the user, and then adds it to the group associated with that user.
- Modifying the group's notify view will affect all users associated with that group.

Instead of specifying the notify view for a group as part of the **snmp-server group** command, use the following commands in the order specified:

1. **snmp-server user**—Configures an SNMP user.
2. **snmp-server group**—Configures an SNMP group, without adding a notify view.
3. **snmp-server host**—Autogenerates the notify view by specifying the recipient of a trap operation.

SNMP Contexts

SNMP contexts provide VPN users with a secure way of accessing MIB data. When a VPN is associated with a context, that VPN's specific MIB data exists in that context. Associating a VPN with a context enables service providers to manage networks with multiple VPNs. Creating and associating a context with a VPN enables a provider to prevent the users of one VPN from accessing information about users of other VPNs on the same networking device.

Use this command with the **context** *context-name* keyword and argument to associate a read, write, or notify SNMP view with an SNMP context.

Examples

Create an SNMP Group

The following example shows how to create the SNMP server group "public," allowing read-only access for all objects to members of the standard named access list "lmnop":

```
Router(config)# snmp-server group public v2c access lmnop
```

Remove an SNMP Server Group

The following example shows how to remove the SNMP server group "public" from the configuration:

```
Router(config)# no snmp-server group public v2c
```

Associate an SNMP Server Group with Specified Views

The following example shows SNMP context "A" associated with the views in SNMPv2c group "GROUP1":

```
Router(config)# snmp-server context A
Router(config)# snmp mib community commA
Router(config)# snmp mib community-map commA context A target-list commAVpn
Router(config)# snmp-server group GROUP1 v2c context A read viewA write viewA notify viewB
```

Related Commands

Command	Description
show snmp group	Displays the names of groups on the router and the security model, the status of the different views, and the storage type of each group.
snmp mib community-map	Associates a SNMP community with an SNMP context, engine ID, security name, or VPN target list.
snmp-server host	Specifies the recipient of a SNMP notification operation.
snmp-server user	Configures a new user to a SNMP group.

snmp-server host

To specify the recipient of a Simple Network Management Protocol (SNMP) notification operation, use the **snmp-server host** command in global configuration mode. To remove the specified host from the configuration, use the **no** form of this command.

snmp-server host {*hostname* | *ip-address*} [**vrf** *vrf-name*] [**informs** | **traps**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*]

no snmp-server host {*hostname* | *ip-address*} [**vrf** *vrf-name*] [**informs** | **traps**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*]

Command Syntax on Cisco ME 3400, ME 3400E, and Catalyst 3750 Metro Switches

snmp-server host *ip-address* {*community-string* | {**informs** | **traps**} {*community-string* | **version** {**1** | **2c** | **3** {**auth** | **noauth**}} *community-string* | **version** {**1** | **2c** | **3** {**auth** | **noauth**}} *community-string* | **vrf** *vrf-name* {**informs** | **traps**} {*community-string* | **version** {**1** | **2c** | **3** {**auth** | **noauth**}} *community-string*}} [*notification-type*]

no snmp-server host *ip-address* {*community-string* | {**informs** | **traps**} {*community-string* | **version** {**1** | **2c** | **3** {**auth** | **noauth**}} *community-string* | **version** {**1** | **2c** | **3** {**auth** | **noauth**}} *community-string* | **vrf** *vrf-name* {**informs** | **traps**} {*community-string* | **version** {**1** | **2c** | **3** {**auth** | **noauth**}} *community-string*}} [*notification-type*]

Command Syntax on Cisco 7600 Series Router

snmp-server host *ip-address* {*community-string* | {**informs** | **traps**} {*community-string* | **version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**}} *community-string* | **version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**}} *community-string* | **vrf** *vrf-name* {**informs** | **traps**} {*community-string* | **version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**}} *community-string*}} [*notification-type*]

no snmp-server host *ip-address* {*community-string* | {**informs** | **traps**} {*community-string* | **version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**}} *community-string* | **version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**}} *community-string* | **vrf** *vrf-name* {**informs** | **traps**} {*community-string* | **version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**}} *community-string*}} [*notification-type*]

Syntax Description

hostname	Name of the host. The SNMP notification host is typically a network management station (NMS) or SNMP manager. This host is the recipient of the SNMP traps or informs.
ip-address	IPv4 address or IPv6 address of the SNMP notification host.
vrf	(Optional) Specifies that a Virtual Private Network (VPN) routing and forwarding (VRF) instance should be used to send SNMP notifications. • In Cisco IOS Release 12.2(54)SE, the **vrf** keyword is required.
vrf-name	(Optional) VPN VRF instance used to send SNMP notifications. • In Cisco IOS Release 12.2(54)SE, the *vrf-name* argument is required.
informs	(Optional) Specifies that notifications should be sent as informs. • In Cisco IOS Release 12.2(54)SE, the **informs** keyword is required.

traps	(Optional) Specifies that notifications should be sent as traps. This is the default. • In Cisco IOS Release 12.2(54)SE, the **traps** keyword is required.
version	(Optional) Specifies the version of the SNMP that is used to send the traps or informs. The default is 1. • In Cisco IOS Release 12.2(54)SE, the **version** keyword is required and the **priv** keyword is not supported. If you use the **version** keyword, one of the following keywords must be specified: • **1**—SNMPv1. • **2c**—SNMPv2C. • **3**—SNMPv3. The most secure model because it allows packet encryption with the **priv** keyword. The default is **noauth**. One of the following three optional security level keywords can follow the **3** keyword: – **auth**—Enables message digest algorithm 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication. – **noauth**—Specifies that the noAuthNoPriv security level applies to this host. This is the default security level for SNMPv3. – **priv**—Enables Data Encryption Standard (DES) packet encryption (also called "privacy").
community-string	Password-like community string sent with the notification operation. **Note** You can set this string using the **snmp-server host** command by itself, but Cisco recommends that you define the string using the **snmp-server community** command prior to using the **snmp-server host** command. **Note** The "at" sign (@) is used for delimiting the context information.
udp-port	(Optional) Specifies that SNMP traps or informs are to be sent to an NMS host. • In Cisco IOS Release 12.2(54)SE, the **udp-port** keyword is not supported.
port	(Optional) User Datagram Protocol (UDP) port number of the NMS host. The default is 162. • In Cisco IOS Release 12.2(54)SE, the *port* argument is not supported.
notification-type	(Optional) Type of notification to be sent to the host. If no type is specified, all available notifications are sent. See the "Notification-Type Keywords" section on page 2218 in the "Usage Guidelines" section for more information about the keywords available.

Command Default

This command behavior is disabled by default. A recipient is not specified to receive notifications.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
Cisco IOS Release 12 Mainline/T Train	
12.0(3)T	• The **version 3** [**auth** | **noauth** | **priv**] syntax was added as part of the SNMPv3 Support feature. • The **hsrp** notification-type keyword was added. • The **voice** notification-type keyword was added.
12.1(3)T	The **calltracker** notification-type keyword was added for the Cisco AS5300 and AS5800 platforms.
12.2(2)T	• The **vrf** *vrf-name* keyword and argument combination was added. • The **ipmobile** notification-type keyword was added. • Support for the **vsimaster** notification-type keyword was added for the Cisco 7200 and Cisco 7500 series.
12.2(4)T	• The **pim** notification-type keyword was added. • The **ipsec** notification-type keyword was added.
12.2(8)T	• The **mpls-traffic-eng** notification-type keyword was added. • The **director** notification-type keyword was added.
12.2(13)T	• The **srp** notification-type keyword was added. • The **mpls-ldp** notification-type keyword was added.
12.3(2)T	• The **flash** notification-type keyword was added. • The **l2tun-session** notification-type keyword was added.
12.3(4)T	• The **cpu** notification-type keyword was added. • The **memory** notification-type keyword was added. • The **ospf** notification-type keyword was added.
12.3(8)T	The **iplocalpool** notification-type keyword was added for the Cisco 7200 and 7301 series routers.
12.3(11)T	The **vrrp** keyword was added.
12.3(14)T	• Support for SNMP over IPv6 transport was integrated into Cisco IOS Release 12.3(14)T. Either an IP or IPv6 Internet address can be specified as the *hostname* argument. • The **eigrp** notification-type keyword was added.
12.4(20)T	The **license** notification-type keyword was added.
15.0(1)M	• The **nhrp** notification-type keyword was added. • The automatic insertion of the **snmp-server community** command into the configuration, along with the community string specified in the **snmp-server host** command, was changed. The **snmp-server community** command must be manually configured.
Cisco IOS Release 12.0S	
12.0(17)ST	The **mpls-traffic-eng** notification-type keyword was added.
12.0(21)ST	The **mpls-ldp** notification-type keyword was added.

Release	Modification
12.0(22)S	• All features in Cisco IOS Release 12.0ST were integrated into Cisco IOS Release 12.0(22)S. • The **mpls-vpn** notification-type keyword was added.
12.0(23)S	The **l2tun-session** notification-type keyword was added.
12.0(26)S	The **memory** notification-type keyword was added.
12.0(27)S	• Support for SNMP over IPv6 transport was added. Either an IP or IPv6 Internet address can be specified as the *hostname* argument. • The **vrf** *vrf-name* keyword and argument combination was added to support multiple Lightweight Directory Protocol (LDP) contexts for VPNs.
12.0(31)S	The **l2tun-pseudowire-status** notification-type keyword was added.
Release 12.2S	
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(25)S	• The **cpu** notification-type keyword was added. • The **memory** notification-type 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.
12.2(31)SB2	The **cef** notification-type keyword was added.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI5	• The **dhcp-snooping** notification-type keyword was added. • The **errdisable** notification-type keyword was added.
12.2(54)SE	This command was modified. See the "Command Syntax on Cisco ME 3400, ME 3400E, and Catalyst 3750 Metro Switches" section on page 2213 for the command syntax for these switches.
12.2(33)SXJ	This command was integrated into Cisco IOS Release 12.2(33)SXJ. The **public storm-control** notification-type keyword was added.
12.2(50)SY	This command integrated into Cisco IOS Release 12.2(50)SY.
Cisco IOS Release 15S	
15.0(1)S	This command was modified. The **flowmon** notification-type keyword was added.
Cisco IOS XE	
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

If you enter this command with no optional keywords, the default is to send all notification-type traps to the host. No informs will be sent to the host.

The **no snmp-server host** command with no keywords disables traps, but not informs, to the host. To disable informs, use the **no snmp-server host informs** command.

Note If a community string is not defined using the **snmp-server community** command prior to using this command, the default form of the **snmp-server community** command will automatically be inserted into the configuration. The password (community string) used for this automatic configuration of the **snmp-server community** will be the same as that specified in the **snmp-server host** command. This automatic command insertion and use of passwords is the default behavior for Cisco IOS Release 12.0(3) and later releases.

SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received. However, an SNMP entity that receives an inform request acknowledges the message with an SNMP response protocol data unit (PDU). If the sender never receives the response, the inform request can be sent again. Thus, informs are more likely than traps to reach their intended destination.

Compared to traps, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Also, traps are sent only once; an inform may be tried several times. The retries increase traffic and contribute to a higher overhead on the network.

If you do not enter an **snmp-server host** command, no notifications are sent. To configure the router to send SNMP notifications, you must enter at least one **snmp-server host** command. If you enter the command with no optional keywords, all trap types are enabled for the host.

To enable multiple hosts, you must issue a separate **snmp-server host** command for each host. You can specify multiple notification types in the command for each host.

When multiple **snmp-server host** commands are given for the same host and kind of notification (trap or inform), each succeeding command overwrites the previous command. Only the last **snmp-server host** command will be in effect. For example, if you enter an **snmp-server host inform** command for a host and then enter another **snmp-server host inform** command for the same host, the second command will replace the first.

The **snmp-server host** command is used in conjunction with the **snmp-server enable** command. Use the **snmp-server enable** command to specify which SNMP notifications are sent globally. For a host to receive most notifications, at least one **snmp-server enable** command and the **snmp-server host** command for that host must be enabled.

Some notification types cannot be controlled with the **snmp-server enable** command. Some notification types are always enabled, and others are enabled by a different command. For example, the **linkUpDown** notifications are controlled by the **snmp trap link-status** command. These notification types do not require an **snmp-server enable** command.

The availability of a notification-type options depends on the router type and the Cisco IOS software features supported on the router. For example, the **envmon** notification type is available only if the environmental monitor is part of the system. To see what notification types are available on your system, use the command help **?** at the end of the **snmp-server host** command.

The **vrf** keyword allows you to specify the notifications being sent to a specified IP address over a specific virtual routing and forwarding (VRF) VPN. The VRF defines a VPN membership of a user so that data is stored using the VPN.

In the case of the NMS sending the query having a correct SNMP community but that does not have a read or a write view, the SNMP agent returns the following error values:

- For a get or a getnext query, returns GEN_ERROR for SNMPv1 and AUTHORIZATION_ERROR for SNMPv2C.
- For a set query, returns NO_ACCESS_ERROR.

Notification-Type Keywords

The notification type can be one or more of the following keywords:

Note The available notification types differ based on the platform and Cisco IOS release. For a complete list of available notification types, use the question mark (?) online help function.

- **aaa server**—Sends SNMP authentication, authorization, and accounting (AAA) traps.
- **adslline**—Sends Asymmetric Digital Subscriber Line (ADSL) LINE-MIB traps.
- **atm**—Sends ATM notifications.
- **authenticate-fail**—Sends an SNMP 802.11 Authentication Fail trap.
- **auth-framework**—Sends SNMP CISCO-AUTH-FRAMEWORK-MIB notifications.
- **bgp**—Sends Border Gateway Protocol (BGP) state change notifications.
- **bridge**—Sends SNMP STP Bridge MIB notifications.
- **bstun**—Sends Block Serial Tunneling (bstun) event notifications.
- **bulkstat**—Sends Data-Collection-MIB notifications.
- **c6kxbar**—Sends SNMP crossbar notifications.
- **callhome**—Sends Call Home MIB notifications.
- **calltracker**—Sends Call Tracker call-start/call-end notifications.
- **casa**—Sends Cisco Appliances Services Architecture (CASA) event notifications.
- **ccme**—Sends SNMP Cisco netManager Event (CCME) traps.
- **cef**—Sends notifications related to Cisco Express Forwarding.
- **chassis**—Sends SNMP chassis notifications.
- **cnpd**—Sends Cisco network-based application recognition (NBAR) Protocol Discovery (CNPD) traps.
- **config**—Sends configuration change notifications.
- **config-copy**—Sends SNMP config-copy notifications.
- **config-ctid**—Sends SNMP config-ctid notifications.
- **cpu**—Sends CPU-related notifications.
- **csg**—Sends SNMP Content Services Gateway (CSG) notifications.
- **deauthenticate**—Sends an SNMP 802.11 Deauthentication trap.
- **dhcp-snooping**—Sends Dynamic Host Configuration Protocol (DHCP) snooping MIB notifications.
- **director**—Sends notifications related to DistributedDirector.
- **disassociate**—Sends an SNMP 802.11 Disassociation trap.
- **dlsw**—Sends data-link switching (DLSW) notifications.
- **dnis**—Sends SNMP Dialed Number Identification Service (DNIS) traps.
- **dot1x**—Sends 802.1X notifications.
- **dot11-mibs**—Sends dot11 traps.
- **dot11-qos**—Sends SNMP 802.11 QoS Change trap.

- **ds1**—Sends SNMP digital signaling 1 (DS1) notifications.
- **ds1-loopback**—Sends ds1-loopback traps.
- **dspu**—Sends downstream physical unit (DSPU) notifications.
- **eigrp**—Sends Enhanced Interior Gateway Routing Protocol (EIGRP) stuck-in-active (SIA) and neighbor authentication failure notifications.
- **energywise**—Sends SNMP energywise notifications.
- **entity**—Sends Entity MIB modification notifications.
- **entity-diag**—Sends SNMP entity diagnostic MIB notifications.
- **envmon**—Sends Cisco enterprise-specific environmental monitor notifications when an environmental threshold is exceeded.
- **errdisable**—Sends error disable notifications.
- **ethernet-cfm**—Sends SNMP Ethernet Connectivity Fault Management (CFM) notifications.
- **event-manager**—Sends SNMP Embedded Event Manager notifications.
- **firewall**—Sends SNMP Firewall traps.
- **flash**—Sends flash media insertion and removal notifications.
- **flexlinks**—Sends FLEX links notifications.
- **flowmon**—Sends flow monitoring notifications.
- **frame-relay**—Sends Frame Relay notifications.
- **fru-ctrl**—Sends entity field-replaceable unit (FRU) control notifications.
- **hsrp**—Sends Hot Standby Routing Protocol (HSRP) notifications.
- **icsudsu**—Sends SNMP ICSUDSU traps.
- **iplocalpool**—Sends IP local pool notifications.
- **ipmobile**—Sends Mobile IP notifications.
- **ipmulticast**—Sends IP multicast notifications.
- **ipsec**—Sends IP Security (IPsec) notifications.
- **isakmp**—Sends SNMP ISAKMP notifications.
- **isdn**—Sends ISDN notifications.
- **l2tc**—Sends SNMP L2 tunnel configuration notifications.
- **l2tun-pseudowire-status**—Sends pseudowire state change notifications.
- **l2tun-session**—Sends Layer 2 tunneling session notifications.
- **license**—Sends licensing notifications as traps or informs.
- **llc2**—Sends Logical Link Control, type 2 (LLC2) notifications.
- **mac-notification**—Sends SNMP MAC notifications.
- **memory**—Sends memory pool and memory buffer pool notifications.
- **module**—Sends SNMP module notifications.
- **module-auto-shutdown**—Sends SNMP module autoshutdown MIB notifications.
- **mpls-fast-reroute**—Sends SNMP Multiprotocol Label Switching (MPLS) traffic engineering fast reroute notifications.

- **mpls-ldp**—Sends MPLS Label Distribution Protocol (LDP) notifications indicating status changes in LDP sessions.
- **mpls-traffic-eng**—Sends MPLS traffic engineering notifications indicating changes in the status of MPLS traffic engineering tunnels.
- **mpls-vpn**—Sends MPLS VPN notifications.
- **msdp**—Sends SNMP Multicast Source Discovery Protocol (MSDP) notifications.
- **mvpn**—Sends multicast VPN notifications.
- **nhrp**—Sends Next Hop Resolution Protocol (NHRP) notifications.
- **ospf**—Sends Open Shortest Path First (OSPF) sham-link notifications.
- **pim**—Sends Protocol Independent Multicast (PIM) notifications.
- **port-security**—Sends SNMP port-security notifications.
- **power-ethernet**—Sends SNMP power Ethernet notifications.
- **public storm-control**—Sends SNMP public storm-control notifications.
- **pw-vc**—Sends SNMP pseudowire virtual circuit (VC) notifications.
- **repeater**—Sends standard repeater (hub) notifications.
- **resource-policy**—Sends CISCO-ERM-MIB notifications.
- **rf**—Sends SNMP RF MIB notifications.
- **rogue-ap**—Sends an SNMP 802.11 Rogue AP trap.
- **rsrb**—Sends remote source-route bridging (RSRB) notifications.
- **rsvp**—Sends Resource Reservation Protocol (RSVP) notifications.
- **rtr**—Sends Response Time Reporter (RTR) notifications.
- **sdlc**—Sends Synchronous Data Link Control (SDLC) notifications.
- **sdllc**—Sends SDLC Logical Link Control (SDLLC) notifications.
- **slb**—Sends SNMP server load balancer (SLB) notifications.
- **snmp**—Sends any enabled RFC 1157 SNMP linkUp, linkDown, authenticationFailure, warmStart, and coldStart notifications.

Note To enable RFC 2233-compliant link up/down notifications, you should use the **snmp server link trap** command.

- **sonet**—Sends SNMP SONET notifications.
- **srp**—Sends Spatial Reuse Protocol (SRP) notifications.
- **stpx**—Sends SNMP STPX MIB notifications.
- **srst**—Sends SNMP Survivable Remote Site Telephony (SRST) traps.
- **stun**—Sends serial tunnel (STUN) notifications.
- **switch-over**—Sends an SNMP 802.11 Standby Switch-over trap.
- **syslog**—Sends error message notifications (Cisco Syslog MIB). Use the **logging history level** command to specify the level of messages to be sent.
- **syslog**—Sends error message notifications (Cisco Syslog MIB). Use the **logging history level** command to specify the level of messages to be sent.

- **tty**—Sends Cisco enterprise-specific notifications when a TCP connection closes.
- **udp-port**—Sends the notification host's UDP port number.
- **vlan-mac-limit**—Sends SNMP L2 control VLAN MAC limit notifications.
- **vlancreate**—Sends SNMP VLAN created notifications.
- **vlandelete**—Sends SNMP VLAN deleted notifications.
- **voice**—Sends SNMP voice traps.
- **vrrp**—Sends Virtual Router Redundancy Protocol (VRRP) notifications.
- **vsimaster**—Sends Virtual Switch Interface (VSI) Master notifications.
- **vswitch**—Sends SNMP virtual switch notifications.
- **vtp**—Sends SNMP VLAN Trunking Protocol (VTP) notifications.
- **wlan-wep**—Sends an SNMP 802.11 Wireless LAN (WLAN) Wired Equivalent Privacy (WEP) trap.
- **x25**—Sends X.25 event notifications.
- **xgcp**—Sends External Media Gateway Control Protocol (XGCP) traps.

SNMP-Related Notification-Type Keywords

The *notification-type* keywords used in the **snmp-server host** command do not always match the keywords used in the corresponding **snmp-server enable traps** command. For example, the notification keyword applicable to Multiprotocol Label Switching Protocol (MPLS) traffic engineering tunnels is specified as **mpls-traffic-eng** (containing two hyphens and no embedded spaces). The corresponding parameter in the **snmp-server enable traps** command is specified as **mpls traffic-eng** (containing an embedded space and a hyphen).

This syntax difference is necessary to ensure that the CLI interprets the *notification-type* keyword of the **snmp-server host** command as a unified, single-word construct, which preserves the capability of the **snmp-server host** command to accept multiple *notification-type* keywords in the command line. The **snmp-server enable traps** commands, however, often use two-word constructs to provide hierarchical configuration options and to maintain consistency with the command syntax of related commands. Table 326 maps some examples of **snmp-server enable traps** commands to the keywords used in the **snmp-server host** command.

Table 326 SNMP-server enable traps Commands and Corresponding Notification Keywords

snmp-server enable traps Command	snmp-server host Command Keyword
snmp-server enable traps l2tun session	l2tun-session
snmp-server enable traps mpls ldp	mpls-ldp
snmp-server enable traps mpls traffic-eng[1]	mpls-traffic-eng
snmp-server enable traps mpls vpn	mpls-vpn

1. *See the Cisco IOS Multiprotocol Label Switching Command Reference* for documentation of this command.

Examples

If you want to configure a unique SNMP community string for traps but prevent SNMP polling access with this string, the configuration should include an access list. The following example shows how to name a community string comaccess and number an access list 10:

```
Router(config)# snmp-server community comaccess ro 10
Router(config)# snmp-server host 192.20.2.160 comaccess
Router(config)# access-list 10 deny any
```

Note The "at" sign (@) is used as a delimiter between the community string and the context in which it is used. For example, specific VLAN information in BRIDGE-MIB may be polled using *community@VLAN-ID* (for example, public@100), where 100 is the VLAN number.

The following example shows how to send RFC 1157 SNMP traps to a specified host named myhost.cisco.com. Other traps are enabled, but only SNMP traps are sent because only **snmp** is specified in the **snmp-server host** command. The community string is defined as comaccess.

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host myhost.cisco.com comaccess snmp
```

The following example shows how to send the SNMP and Cisco environmental monitor enterprise-specific traps to address 192.30.2.160 using the community string public:

```
Router(config)# snmp-server enable traps snmp
Router(config)# snmp-server enable traps envmon
Router(config)# snmp-server host 192.30.2.160 public snmp envmon
```

The following example shows how to enable the router to send all traps to the host myhost.cisco.com using the community string public:

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host myhost.cisco.com public
```

The following example will not send traps to any host. The BGP traps are enabled for all hosts, but only the ISDN traps are enabled to be sent to a host. The community string is defined as public.

```
Router(config)# snmp-server enable traps bgp
Router(config)# snmp-server host myhost.cisco.com public isdn
```

The following example shows how to enable the router to send all inform requests to the host myhost.cisco.com using the community string public:

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

The following example shows how to send HSRP MIB informs to the host specified by the name myhost.cisco.com. The community string is defined as public.

```
Router(config)# snmp-server enable traps hsrp
Router(config)# snmp-server host myhost.cisco.com informs version 2c public hsrp
```

The following example shows how to send all SNMP notifications to example.com over the VRF named trap-vrf using the community string public:

```
Router(config)# snmp-server host example.com vrf trap-vrf public
```

The following example shows how to configure an IPv6 SNMP notification server with the IPv6 address 2001:0DB8:0000:ABCD:1 using the community string public:

```
Router(config)# snmp-server host 2001:0DB8:0000:ABCD:1 version 2c public udp-port 2012
```

The following example shows how to specify VRRP as the protocol using the community string public:

```
Router(config)# snmp-server enable traps vrrp
Router(config)# snmp-server host myhost.cisco.com traps version 2c public vrrp
```

The following example shows how to send all Cisco Express Forwarding informs to the notification receiver with the IP address 192.40.3.130 using the community string public:

```
Router(config)# snmp-server enable traps cef
Router(config)# snmp-server host 192.40.3.130 informs version 2c public cef
```

The following example shows how to enable all NHRP traps, and how to send all 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
```

Related Commands

Command	Description
show snmp host	Displays recipient details configured for SNMP notifications.
snmp-server enable peer-trap poor qov	Enables poor quality of voice notifications for applicable calls associated with a specific voice dial peer.
snmp-server enable traps	Enables SNMP notifications (traps and informs).
snmp-server enable traps nhrp	Enables SNMP notifications (traps) for NHRP.
snmp-server informs	Specifies inform request options.
snmp-server link trap	Enables linkUp/linkDown SNMP trap that are compliant with RFC 2233.
snmp-server trap-source	Specifies the interface from which an SNMP trap should originate.
snmp-server trap-timeout	Defines how often to try resending trap messages on the retransmission queue.
test snmp trap storm-control event-rev1	Tests SNMP storm-control traps.

snmp-server user

To configure a new user to a Simple Network Management Protocol (SNMP) group, use the **snmp-server user** command in global configuration mode. To remove a user from an SNMP group, use the **no** form of this command.

snmp-server user *username group-name* [**remote** *host* [**udp-port** *port*] [**vrf** *vrf-name*]] {**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password*]} [**access** [**ipv6** *nacl*] [**priv** {**des** | **3des** | **aes** {**128** | **192** |**256**}} *privpassword*] {*acl-number* | *acl-name*}]

no snmp-server user *username group-name* [**remote** *host* [**udp-port** *port*] [**vrf** *vrf-name*]] {**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password*]} [**access** [**ipv6** *nacl*] [**priv** {**des** | **3des** | **aes** {**128** | **192** |**256**}} *privpassword*] {*acl-number* | *acl-name*}]

Syntax Description

username	Name of the user on the host that connects to the agent.
group-name	Name of the group to which the user belongs.
remote	(Optional) Specifies a remote SNMP entity to which the user belongs, and the hostname or IPv6 address or IPv4 IP address of that entity. If both an IPv6 address and IPv4 IP address are being specified, the IPv6 host must be listed first.
host	(Optional) Name or IP address of the remote SNMP host.
udp-port	(Optional) Specifies the User Datagram Protocol (UDP) port number of the remote host.
port	(Optional) Integer value that identifies the UDP port. The default is 162.
vrf	(Optional) Specifies an instance of a routing table.
vrf-name	(Optional) Name of the Virtual Private Network (VPN) routing and forwarding (VRF) table to use for storing data.
v1	Specifies that SNMPv1 should be used.
v2c	Specifies that SNMPv2c should be used.
v3	Specifies that the SNMPv3 security model should be used. Allows the use of the **encrypted** keyword or **auth** keyword or both.
encrypted	(Optional) Specifies whether the password appears in encrypted format.
auth	(Optional) Specifies which authentication level should be used.
md5	(Optional) Specifies the HMAC-MD5-96 authentication level.
sha	(Optional) Specifies the HMAC-SHA-96 authentication level.
auth-password	(Optional) String (not to exceed 64 characters) that enables the agent to receive packets from the host.
access	(Optional) Specifies an Access Control List (ACL) to be associated with this SNMP user.
ipv6	(Optional) Specifies an IPv6 named access list to be associated with this SNMP user.
nacl	(Optional) Name of the ACL. IPv4, IPv6, or both IPv4 and IPv6 access lists may be specified. If both are specified, the IPv6 named access list must appear first in the statement.
priv	(Optional) Specifies the use of the User-based Security Model (USM) for SNMP version 3 for SNMP message level security.

des	(Optional) Specifies the use of the 56-bit Digital Encryption Standard (DES) algorithm for encryption.
3des	(Optional) Specifies the use of the 168-bit 3DES algorithm for encryption.
aes	(Optional) Specifies the use of the Advanced Encryption Standard (AES) algorithm for encryption.
128	(Optional) Specifies the use of a 128-bit AES algorithm for encryption.
192	(Optional) Specifies the use of a 192-bit AES algorithm for encryption.
256	(Optional) Specifies the use of a 256-bit AES algorithm for encryption.
privpassword	(Optional) String (not to exceed 64 characters) that specifies the privacy user password.
acl-number	(Optional) Integer in the range from 1 to 99 that specifies a standard access list of IP addresses.
acl-name	(Optional) String (not to exceed 64 characters) that is the name of a standard access list of IP addresses.

Command Default

See Table 327 in the "Usage Guidelines" section for default behaviors for encryption, passwords, and access lists.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.3(2)T	Support for named standard access lists was added.
12.0(27)S	The **ipv6** keyword and *nacl* argument were added to allow for configuration of IPv6 named access lists and IPv6 remote hosts.
12.3(14)T	The **ipv6** keyword and *nacl* argument were integrated into Cisco IOS Release 12.3(14)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	The **priv** keyword and associated arguments were added to enable the use of the USM for SNMP version 3 for SNMP message level security.
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.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Aggregation Services Routers.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

To configure a remote user, specify the IP address or port number for the remote SNMP agent of the device where the user resides. Also, before you configure remote users for a particular agent, configure the SNMP engine ID, using the **snmp-server engineID** command with the **remote** keyword. The remote agent's SNMP engine ID is needed when computing the authentication and privacy digests from the password. If the remote engine ID is not configured first, the configuration command will fail.

For the *privpassword* and *auth-password* arguments, the minimum length is one character; the recommended length is at least eight characters, and should include both letters and numbers.

Table 327 describes the default user characteristics for encryption, passwords, and access lists.

Table 327 snmp-server user Default Descriptions

Characteristic	Default
Access lists	Access from all IP access lists is permitted.
Encryption	Not present by default. The **encrypted** keyword is used to specify that the passwords are message digest algorithm 5 (MD5) digests and not text passwords.
Passwords	Assumed to be text strings.
Remote users	All users are assumed to be local to this SNMP engine unless you specify they are remote with the **remote** keyword.

SNMP passwords are localized using the SNMP engine ID of the authoritative SNMP engine. For informs, the authoritative SNMP agent is the remote agent. You need to configure the remote agent's SNMP engine ID in the SNMP database before you can send proxy requests or informs to it.

Note Changing the engine ID after configuring the SNMP user, does not allow to remove the user. To remove the user, you need to first reconfigure the SNMP user.

Working with Passwords and Digests

No default values exist for authentication or privacy algorithms when you configure the command. Also, no default passwords exist. The minimum length for a password is one character, although Cisco recommends using at least eight characters for security. If you forget a password, you cannot recover it and will need to reconfigure the user. You can specify either a plain-text password or a localized MD5 digest.

If you have the localized MD5 or Secure Hash Algorithm (SHA) digest, you can specify that string instead of the plain-text password. The digest should be formatted as aa:bb:cc:dd where aa, bb, and cc are hexadecimal values. Also, the digest should be exactly 16 octets long.

Examples

The following example shows how to add the user abcd to the SNMP server group named public. In this example, no access list is specified for the user, so the standard named access list applied to the group applies to the user.

```
Router(config)# snmp-server user abcd public v2c
```

The following example shows how to add the user abcd to the SNMP server group named public. In this example, access rules from the standard named access list qrst apply to the user.

```
Router(config)# snmp-server user abcd public v2c access qrst
```

In the following example, the plain-text password cisco123 is configured for the user abcd in the SNMP server group named public:

```
Router(config)# snmp-server user abcd public v3 auth md5 cisco123
```

When you enter a **show running-config** command, a line for this user will be displayed. To learn if this user has been added to the configuration, use the **show snmp user** command.

Note The **show running-config** command does not display any of the active SNMP users created in authPriv or authNoPriv mode, though it does display the users created in noAuthNoPriv mode. To display any active SNMPv3 users created in authPriv, authNoPrv, or noAuthNoPriv mode, use the **show snmp user** command.

If you have the localized MD5 or SHA digest, you can specify that string instead of the plain-text password. The digest should be formatted as aa:bb:cc:dd where aa, bb, and cc are hexadecimal values. Also, the digest should be exactly 16 octets long.

In the following example, the MD5 digest string is used instead of the plain-text password:

```
Router(config)# snmp-server user abcd public v3 encrypted auth md5
00:11:22:33:44:55:66:77:88:99:AA:BB:CC:DD:EE:FF
```

In the following example, the user abcd is removed from the SNMP server group named public:

```
Router(config)# no snmp-server user abcd public v2c
```

In the following example, the user abcd from the SNMP server group named public specifies the use of the 168-bit 3DES algorithm for privacy encryption with secure3des as the password.

```
Router(config)# snmp-server user abcd public priv v2c 3des secure3des
```

Related Commands

Command	Description
show running-config	Displays the contents of the currently running configuration file or the configuration for a specific interface, or map class information.
show snmp user	Displays information on each SNMP username in the group username table.
snmp-server engineID	Displays the identification of the local SNMP engine and all remote engines that have been configured on the router.

snmp trap link-status

To enable Simple Network Management Protocol (SNMP) link trap generation, use the **snmp trap link-status** command in either interface configuration mode or service instance configuration mode. To disable SNMP link traps, use the **no** form of this command.

snmp trap link-status [**permit duplicates**]

no snmp trap link-status [permit duplicates]

Syntax Description.

permit duplicates	(Optional) Permits duplicate SNMP linkup and linkdown traps.

Command Default

SNMP link traps are sent when an interface goes up or down.

Command Modes

Interface configuration (config-if)
Service instance configuration (config-if-srv)

Command History

Release	Modification
10.0	This command was introduced.
12.2(30)S	The **permit duplicates** keyword pair was added in Cisco IOS Release 12.2(30)S.
12.3(8)T	Support for the **permit duplicates** keyword pair was integrated in Cisco IOS Release 12.3(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.
12.2(33)SB	This command's behavior was modified on the Cisco 10000 series router for the PRE3 and PRE4 as described in the Usage Guidelines.
12.2(33)SRD1	Support for this command was extended to service instance configuration mode in Cisco IOS Release 12.2(33)SRD1.

Usage Guidelines

By default, SNMP link traps are sent when an interface goes up or down. For interfaces expected to go up and down during normal usage, such as ISDN interfaces, the output generated by these traps may not be useful. The **no** form of this command disables these traps.

The **permit** and **duplicates** keywords are used together and cannot be used individually. Use the **permit duplicates** keyword pair when an interface is not generating SNMP linkup traps, linkdown traps, or both. When the **snmp trap link-status permit duplicates** command is configured, more than one trap may be sent for the same linkup or linkdown transition.

The **permit duplicates** keyword pair does not guarantee that SNMP link traps will be generated nor should configuring these keywords be required to receive traps.

By default, in service instance configuration mode SNMP link traps are not sent. Also, the **permit duplicates** keyword pair is not available in service instance configuration mode.

Cisco 10000 Series Router Usage Guidelines

In Cisco IOS Release 12.2(33)SB, the **virtual-template snmp** command has a new default configuration. Instead of being enabled by default, **no virtual-template snmp** is the default configuration. This setting enhances scaling and prevents large numbers of entries in 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

The following example shows how to disable SNMP link traps related to the ISDN BRI 0 interface:

```
Router(config)# interface bri 0
Router(config-if)# no snmp trap link-status
```

The following example shows how to enable SNMP link traps for service instance 50 on Ethernet interface 0/1:

```
Router(config)# interface ethernet 0/1
Router(config-if)# service instance 50 ethernet
Router(config-if-srv)# snmp trap link-status
Router(config-if-srv)# exit
```

Related Commands

Command	Description
virtual-template snmp	Allows virtual access interfaces to register with SNMP when they are created or reused.

sntp address

To specify the IPv6 Simple Network Time Protocol (SNTP) server address list to be sent to the client, use the **sntp address** command in DHCP for IPv6 pool configuration mode. To remove the SNTP server address list, use the **no** form of the command.

sntp address *ipv6-address*

no sntp address *ipv6-address*

Syntax Description

ipv6-address	The IPv6 SNTP address of a server to be sent to the client.

Command Default

No SNTP server address is specified.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was updated. It was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

The Dynamic Host Configuration Protocol (DHCP) for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The SNTP server address list option provides a list of one or more IPv6 addresses of SNTP servers available to the client for synchronization. The clients use these SNTP servers to synchronize their system time to that of the standard time servers.

Clients must treat the list of SNTP servers as an ordered list, and the server may list the SNTP servers in decreasing order of preference. The option defined in this document can be used only to configure information about SNTP servers that can be reached using IPv6.

The SNTP server option code is 31. For more information on DHCP options and suboptions, see the "DHCP Options" appendix in the *Network Registrar User's Guide*, Release 6.2.

Examples

The following example shows how to specify the SNTP server address:

```
sntp address 300::1
```

Related Commands

Command	Description
import sntp address	Imports the SNTP server option to a DHCP for IPv6 client.

spd extended-headroom

To configure Selective Packet Discard (SPD) extended headroom, use the **spd extended-headroom** command in global configuration mode. To return to the default value, use the **no** form of this command.

spd extended-headroom *size*

no spd extended-headroom

Syntax Description

size	SPD headroom size, in number of packets.

Command Default

The SPD extended headroom default is 10 packets.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T.

Usage Guidelines

Because Interior Gateway Protocols (IGPs) and link stability are tenuous and crucial, such packets are given the highest priority and are given extended SPD headroom with a default of 10 packets. These packets are not dropped if the size of the input hold queue is lower than 185 (input queue default size + SPD headroom size + SPD extended headroom).

Examples

The following example shows how to configure SPD extended headroom to be 11 packets:

```
Router(config)# spd extended-headroom 11
```

Related Commands

Command	Description
show ipv6 spd	Displays the IPv6 SPD configuration.
spd headroom	Configures SPD headroom.

spd headroom

To configure Selective Packet Discard (SPD) headroom, use the **spd headroom** command in global configuration mode. To return to the default value, use the **no** form of this command.

spd headroom *size*

no spd headroom

Syntax Description

size	SPD headroom size, in number of packets.

Command Default

The SPD headroom default is 100 packets.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T.

Usage Guidelines

SPD prioritizes IPv6 packets with a precedence of 7 by allowing the software to queue them into the process level input queue above the normal input queue limit. The number of packets allowed in excess of the normal limit is called the SPD headroom, the default being 100, which means that a high precedence packet is not dropped if the size of the input hold queue is lower than 175 (input queue default size + SPD headroom size).

Examples

The following example shows how to configure SPD headroom to be 95 packets:

```
Router(config)# spd headroom 95
```

Related Commands

Command	Description
show ipv6 spd	Displays the IPv6 SPD configuration.
spd extended-headroom	Configures SPD extended headroom.

spf-interval (IPv6)

To configure how often Cisco IOS software performs the shortest path first (SPF) calculation, use the **spf-interval** command in address family configuration mode. To restore the default interval, use the **no** form of this command.

spf-interval [**level-1** | **level-2**] *seconds* [*initial-wait*] [*secondary-wait*]

no spf-interval *seconds*

Syntax Description

level-1	(Optional) Summarizes only routes redistributed into Level 1 with the configured prefix value.
level-2	(Optional) Summarizes routes learned by Level 1 routing into the Level 2 backbone with the configured prefix value. Redistributed routes into Level 2 IS-IS also are summarized.
seconds	Minimum amount of time between SPF calculations, in seconds. It can be a number from 1 to 120. The default is 5 seconds.
initial-wait	(Optional) Length of time before the first SPF calculation in milliseconds.
secondary-wait	(Optional) Minimum length of time between the first and second SPF calculation, in milliseconds.

Command Default

The default is 5 seconds.

Command Modes

Address family configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
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.
12.2(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 2.6	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

SPF calculations are performed only when the topology changes. They are not performed when external routes change.

The **spf-interval** (IPv6) command controls how often Cisco IOS software can perform the SPF calculation. The SPF calculation is processor-intensive. Therefore, it may be useful to limit how often the SPF calculation is performed, especially when the area is large and the topology changes often. Increasing the SPF interval reduces the processor load of the router, but it could slow down the rate of convergence.

If IPv6 and IPv4 are configured on the same interface, they must be running the same Intermediate System-to-Intermediate System (IS-IS) level.

You can use the **spf-interval** (IPv6) command only when using the IS-IS multitopology support for IPv6 feature.

Examples

The following example sets the SPF calculation interval to 30 seconds:

```
Router(config)# router isis
Router(config-router)# address-family ipv6
Router(config-router-af)# spf-interval 30
```

Related Commands

Command	Description
prc-interval (IPv6)	Controls the hold-down period between PRCs.

split-horizon (IPv6 RIP)

To configure split horizon processing of IPv6 Routing Information Protocol (RIP) router updates, use the **split-horizon** command in router configuration mode. To disable the split horizon processing of IPv6 RIP updates, use the **no** form of this command.

split-horizon

no split-horizon

Syntax Description

This command has no arguments or keywords.

Command Default

Split horizon is configured and active by default. However, for ATM interfaces and subinterfaces **split-horizon** is disabled by default.

Command Modes

Router configuration

Command History

Release	Modification
12.2(2)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 Release 12.2(14)S.
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.
12.2(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 **split-horizon** (IPv6 RIP) command is similar to the **ip split-horizon** command, except that it is IPv6-specific.

This command configures split horizon processing of IPv6 RIP router updates. When split horizon is configured, the advertisement of networks out the interfaces from which the networks are learned is suppressed.

If both split horizon and poison reverse are configured, then split horizon behavior is replaced by poison reverse behavior (routes learned via RIP are advertised out the interface over which they were learned, but with an unreachable metric).

Note In general, changing the state of the default for the **split-horizon** command is not recommended, unless you are certain that your application requires a change in order to properly advertise routes. If split horizon is disabled on a serial interface (and that interface is attached to a packet-switched network), you *must* disable split horizon for all routers and access servers in any relevant multicast groups on that network.

Examples

The following example configures split horizon processing for the IPv6 RIP routing process named cisco:

```
Router(config)# ipv6 router rip cisco
Router(config-rtr)# split-horizon
```

Related Commands

Command	Description
neighbor (RIP)	Defines a neighboring router with which to exchange routing information.

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.

standby ipv6

To activate the Hot Standby Router Protocol (HSRP) in IPv6, use the **standby ipv6** command in interface configuration mode. To disable HSRP, use the **no** form of this command.

standby [*group-number*] **ipv6** {*ipv6-global-address* | *ipv6-address*/*prefix-length* | *ipv6-prefix*/*prefix-length* | *link-local-address* | **autoconfig**}

no standby [*group-number*] **ipv6** {*ipv6-global-address* | *ipv6-address*/*prefix-length* | *ipv6-prefix*/*prefix-length* | *link-local-address* | **autoconfig**}

Syntax Description

group-number	(Optional) Group number on the interface for which HSRP is being activated. The default is 0. The group number range is from 0 to 255 for HSRP version 1 and from 0 to 4095 for HSRP version 2.
ipv6-global-address	IPv6 address of the hot standby router interface.
ipv6-prefix	The IPv6 network assigned to the interface. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/prefix-length	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
link-local-address	Link-local address of the hot standby router interface.
autoconfig	Indicates that a virtual link-local address will be generated automatically from the link-local prefix and a modified EUI-64 format interface identifier, where the EUI-64 interface identifier is created from the relevant HSRP virtual MAC address.

Command Default

The default group number is 0.
HSRP is disabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(4)T	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.
12.2(33)SXI4	Users can configure a fully routable global virtual IPv6 address.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

An Ethernet or FDDI type interface must be used for HSRP for IPv6. HSRP version 2 must be enabled on an interface before HSRP IPv6 can be configured.

The **standby ipv6** command enables an HSRP group for IPv6 operation. If the **autoconfig** keyword is used, then a link-local address will be generated from the link-local prefix and a modified EUI-64 format interface identifier, where the EUI-64 interface identifier is created from the relevant HSRP virtual MAC address.

If an IPv6 global address is used, it must include an IPv6 prefix length. If a link-local address is used, it does not have a prefix.

Examples

The following example enables an HSRP group for IPv6 operation:

```
Router(config)# standby version 2
Router(config)# interface ethernet 0
Router(config-if)# standby ipv6 autoconfig
```

The following example shows three HSRP global IPv6 addresses with an explicitly configured link-local address:

```
interface Ethernet0/0
 no ip address
 ipv6 address 2001::0DB8:1/64
 standby version 2
 standby 1 ipv6 FE80::1:CAFÉ
 standby 1 ipv6 2001::0DB8:2/64
 standby 1 ipv6 2001:0DB8::3/64
 standby 1 ipv6 2001:0DB8::4/64
```

Related Commands

Command	Description
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

standby preempt

To configure Hot Standby Router Protocol (HSRP) preemption and preemption delay, use the **standby preempt** command in interface configuration mode. To restore the default values, use the **no** form of this command.

standby [*group-number*] **preempt** [**delay** {**minimum** *seconds* | **reload** *seconds* | **sync** *seconds*}]

no standby [*group-number*] **preempt** [**delay** {**minimum** *seconds* | **reload** *seconds* | **sync** *seconds*}]

Syntax Description

group-number	(Optional) Group number on the interface to which the other arguments in this command apply.
delay	(Optional) Required if either the **minimum**, **reload**, or **sync** keywords are specified.
minimum *seconds*	(Optional) Specifies the minimum delay period in seconds. The *seconds* argument causes the local router to postpone taking over the active role for a minimum number of seconds since that router was last restarted. The range is from 0 to 3600 seconds (1 hour). The default is 0 seconds (no delay).
reload *seconds*	(Optional) Specifies the preemption delay, in seconds, after a reload only. This delay period applies only to the first interface-up event after the router has reloaded.
sync *seconds*	(Optional) Specifies the maximum synchronization period for IP redundancy clients in seconds.

Command Default

The default group number is 0.
The default delay is 0 seconds; if the router wants to preempt, it will do so immediately.
By default, the router that comes up later becomes the standby.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.3	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.
12.0(2)T	The **minimum** and **sync** keywords were added.
12.2	The behavior of the command changed such that **standby preempt** and **standby priority** must be entered as separate commands.
12.2	The **reload** keyword 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.

Release	Modification
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	The behavior of the command changed such that **standby preempt** and **standby priority** must be entered as separate commands.

Usage Guidelines

Note Cisco IOS 12.2SX software releases earlier than Cisco IOS Release 12.2(33)SXH use the syntax from Cisco IOS Release 12.1, which supports **preempt** as a keyword for the **standby priority** command. Cisco IOS Release 12.2(33)SXH and later releases use Cisco IOS Release 12.2 syntax, which requires **standby preempt** and **standby priority** to be entered as separate commands.

When the **standby preempt** command is configured, the router is configured to preempt, which means that when the local router has a Hot Standby priority higher than the current active router, the local router should attempt to assume control as the active router. If preemption is not configured, the local router assumes control as the active router only if it receives information indicating no router is in the active state (acting as the designated router).

This command is separate from the **standby delay minimum reload** interface configuration command, which delays HSRP groups from initializing for the specified time after the interface comes up.

When a router first comes up, it does not have a complete routing table. If it is configured to preempt, it will become the active router, yet it is unable to provide adequate routing services. Solve this problem by configuring a delay before the preempting router actually preempts the currently active router.

When group number 0 is used, no group number is written to NVRAM, providing backward compatibility.

IP redundancy clients can prevent preemption from taking place. The **standby preempt delay sync** *seconds* command specifies a maximum number of seconds to allow IP redundancy clients to prevent preemption. When this expires, then preemption takes place regardless of the state of the IP redundancy clients.

The **standby preempt delay reload** *seconds* command allows preemption to occur only after a router reloads. This provides stabilization of the router at startup. After this initial delay at startup, the operation returns to the default behavior.

The **no standby preempt delay** command will disable the preemption delay but preemption will remain enabled. The **no standby preempt delay minimum** *seconds* command will disable the minimum delay but leave any synchronization delay if it was configured.

When the **standby follow** command is used to configure an HSRP group to become an IP redundancy client of another HSRP group, the client group takes its state from the master group it is following. Therefore, the client group does not use its timer, priority, or preemption settings. A warning is displayed if these settings are configured on a client group:

```
Router(config-if)# standby 1 preempt delay minimum 300
% Warning: This setting has no effect while following another group.
```

Examples

In the following example, the router will wait for 300 seconds (5 minutes) before attempting to become the active router:

```
Router(config)# interface ethernet 0
Router(config-if)# standby ip 172.19.108.254
```

```
Router(config-if)# standby preempt delay minimum 300
```

standby priority

To configure Hot Standby Router Protocol (HSRP) priority, use the **standby priority** command in interface configuration mode. To restore the default values, use the **no** form of this command.

standby [*group-number*] **priority** *priority*

no standby [*group-number*] **priority** *priority*

Syntax Description

group-number	(Optional) Group number on the interface to which the other arguments in this command apply. The default group number is 0.
priority	Priority value that prioritizes a potential Hot Standby router. The range is from 1 to 255, where 1 denotes the lowest priority and 255 denotes the highest priority. The default priority value is 100. The router in the HSRP group with the highest priority value becomes the active router.

Command Default

The default group number is 0.
The default priority is 100.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.3	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.
12.2	The behavior of the command changed such that **standby preempt** and **standby priority** must be entered as separate commands.
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(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	The behavior of the command changed such that **standby preempt** and **standby priority** must be entered as separate commands.

Usage Guidelines

Note Cisco IOS 12.2SX software releases earlier than Cisco IOS Release 12.2(33)SXH use the syntax from Cisco IOS Release 12.1, which supports **preempt** as a keyword for the **standby priority** command. Cisco IOS Release 12.2(33)SXH and later releases use Cisco IOS Release 12.2 syntax, which requires **standby preempt** and **standby priority** to be entered as separate commands.

When group number 0 is used, the number 0 is written to NVRAM, providing backward compatibility.

The assigned priority is used to help select the active and standby routers. Assuming that preemption is enabled, the router with the highest priority becomes the designated active router. In case of ties, the primary IP addresses are compared, and the higher IP address has priority.

Note that the priority of the device can change dynamically if an interface is configured with the **standby track** command and another interface on the router or a tracked object goes down.

When the **standby follow** command is used to configure an HSRP group to become an IP redundancy client of another HSRP group, the client group takes its state from the master group it is following. Therefore, the client group does not use its timer, priority, or preemption settings. A warning is displayed if these settings are configured on a client group:

```
Router(config-if)# standby 1 priority 110
%Warning: This setting has no effect while following another group.
```

Examples

In the following example, the router has a priority of 120 (higher than the default value):

```
Router(config)# interface ethernet 0
Router(config-if)# standby ip 172.19.108.254
Router(config-if)# standby priority 120
Router(config-if)# standby preempt delay 300
```

Related Commands

Command	Description
standby track	Configures an interface so that the Hot Standby priority changes based on the availability of other interfaces.

standby version

To change the version of the Hot Standby Router Protocol (HSRP), use the **standby version** command in interface configuration mode. To change to the default version, use the **no** form of this command.

standby version {**1** | **2**}

no standby version

Syntax Description

1	Specifies HSRP version 1.
2	Specifies HSRP version 2.

Command Default

HSRP version 1 is the default HSRP version.

Command Modes

Interface configuration (config-if)

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(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 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

HSRP version 2 addresses limitations of HSRP version 1 by providing an expanded group number range of 0 to 4095.

HSRP version 2 does not interoperate with HSRP version 1. An interface cannot operate both version 1 and version 2 because both versions are mutually exclusive. However, the different versions can be run on different physical interfaces of the same router. The group number range is from 0 to 255 for HSRP version 1 and from 0 to 4095 for HSRP version 2. You cannot change from version 2 to version 1 if you have configured groups above 255. Use the **no standby version** command to set the HSRP version to the default version, version 1.

If an HSRP version is changed, each group will reinitialize because it now has a new virtual MAC address.

Examples

The following example shows how to configure HSRP version 2 on an interface with a group number of 500:

```
Router(config)# interface vlan500
Router(config-if)# standby version 2
Router(config-if)# standby 500 ip 172.20.100.10
Router(config-if)# standby 500 priority 110
Router(config-if)# standby 500 preempt
Router(config-if)# standby 500 timers 5 15
```

Related Commands

Command	Description
show standby	Displays HSRP information.

stub

Note Effective with Cisco IOS Release 15.0(1)M and 12.2(33)SRE, the **stub** command was replaced by the **eigrp stub** command. See the **eigrp stub** command for more information.

To configure a router as a stub using Enhanced Interior Gateway Routing Protocol (EIGRP), use the **stub** command in router configuration mode. To disable the EIGRP stub routing feature, use the **no** form of this command.

stub [**receive-only** | **connected** | **static** | **summary** | **redistributed**]

no stub [**receive-only** | **connected** | **static** | **summary** | **redistributed**]

Syntax Description

receive-only	(Optional) Sets the router as a receive-only neighbor.
connected	(Optional) Advertises connected routes.
static	(Optional) Advertises static routes.
summary	(Optional) Advertises summary routes.
redistributed	(Optional) Advertises redistributed routes from other protocols and autonomous systems.

Command Default

Stub routing is not enabled.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
12.4(6)T	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.
15.0(1)M	This command was replaced by the **eigrp stub** command.
12.2(33)SRE	This command was replaced by the **eigrp stub** command.

Usage Guidelines

Use the **stub** command to configure a router as a stub where the router directs all IPv6 traffic to a distribution router.

The **stub** command can be modified with keywords, and more than one keyword can be used in the same syntax. These options can be used in any combination, except for the **receive-only** keyword. The **receive-only** keyword will restrict the router from sharing any of its routes with any other router in that EIGRP autonomous system, and the **receive-only** keyword will not permit any other option to be specified because it prevents any type of route from being sent. The **connected**, **static**, **summary**, and **redistributed** keywords can be used in any combination but cannot be used with the **receive-only** keyword.

If any of these four keywords is used with the **stub** command, only the route types specified by the particular keywords will be sent. Route types specified by the nonused keywords will not be sent.

The **connected** keyword permits the EIGRP stub routing feature to send connected routes. If the connected routes are not covered by a network statement, it may be necessary to redistribute connected routes with the **redistribute connected** command under the EIGRP process. This option is enabled by default.

The **static** keyword permits the EIGRP stub routing feature to send static routes. Without the configuration of this option, EIGRP will not send any static routes, including internal static routes that normally would be automatically redistributed. It will still be necessary to redistribute static routes with the **redistribute static** command.

The **summary** keyword permits the EIGRP stub routing feature to send summary routes. Summary routes can be created manually with the **ipv6 summary address eigrp** command or automatically at a major network border router with the **auto-summary** command enabled. This option is enabled by default.

The **redistributed** keyword permits the EIGRP stub routing feature to send other routing protocols and autonomous systems. Without the configuration of this option, EIGRP will not advertise redistributed routes.

Note Multiaccess interfaces such as ATM, Ethernet, Frame Relay, ISDN PRI, and X.25 are supported by the EIGRP stub routing feature only when all routers on that interface, except the hub, are configured as stub routers.

Examples

In the following example, the **stub** command is used to configure the router as a stub that advertises connected and summary routes:

```
ipv6 router eigrp 1
 network 3FEE:12E1:2AC1:EA32::/64
 stub
```

In the following example, the **stub** command is issued with the **connected** and **static** keywords to configure the router as a stub that advertises connected and static routes (sending summary routes will not be permitted):

```
ipv6 router eigrp 1
 network 3FEE:12E1:2AC1:EA32::/64
 stub connected static
```

In the following example, the **stub** command is issued with the **receive-only** keyword to configure the router as a receive-only neighbor (connected, summary, and static routes will not be sent):

```
ipv6 router eigrp 1
 network 3FEE:12E1:2AC1:EA32::/64 eigrp
 stub receive-only
```

In the following example, the **stub** command is issued with the **redistributed** keyword to configure the router to advertise other protocols and autonomous systems:

```
ipv6 router eigrp 1
 network 3FEE:12E1:2AC1:EA32::/64 eigrp
 stub redistributed
```

Related Commands

Command	Description
auto-summary (EIGRP)	Allows automatic summarization of subnet routes into network-level routes.
ipv6 summary-address eigrp	Configures a summary aggregate address for a specified interface.
redistribute (IPv6)	Redistributes IPv6 routes from one routing domain into another routing domain.

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.

summary-prefix (IPv6 IS-IS)

To create aggregate IPv6 prefixes for Intermediate System-to-Intermediate System (IS-IS), use the **summary-prefix** command in address family configuration mode. To restore the default, use the **no** form of this command.

summary-prefix *ipv6-prefix*/*prefix-length* {**level-1** | **level-1-2** | **level-2**}

no summary-prefix *ipv6-prefix*/*prefix-length* {**level-1** | **level-1-2** | **level-2**}

Syntax Description

ipv6-prefix	Summary prefix designated for a range of IPv6 prefixes. The *ipv6-prefix* argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/prefix-length	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
level-1	Only routes redistributed into Level 1 are summarized with the configured prefix value.
level-1-2	Summary routes are applied when redistributing routes into Level 1 and Level 2 IS-IS, and when Level 2 IS-IS advertises Level 1 routes reachable in its area.
level-2	Routes learned by Level 1 routing are summarized into the Level 2 backbone with the configured prefix value. Redistributed routes into Level 2 IS-IS will be summarized also.

Command Default

All redistributed routes are advertised individually.

Command Modes

Address family configuration

Command History

Release	Modification
12.2(8)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 Release 12.2(14)S.
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.
12.2(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 2.4	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

Multiple groups of prefixes can be summarized for a given level. Routes learned from other routing protocols can also be summarized. The metric used to advertise the summary is the smallest metric of all the more specific routes. This command helps reduce the size of the routing updates generated by the router, resulting in smaller routing tables on neighbor routers.

This command also reduces the size of the link-state packets (LSPs) and thus the link-state database (LSDB). It also helps ensure stability because a summary advertisement is depending on many more specific routes. If one more specific route flaps, in most cases this flapping does not cause a flap of the summary advertisement.

The drawback of summary prefixes is that other routes might have less information with which to calculate the most optimal routing table for all individual destinations.

Note When IS-IS advertises a summary prefix, it automatically inserts the summary prefix into the IPv6 routing table but labels it as a "discard" route entry. Any packet that matches the entry will be discarded to prevent routing loops. When IS-IS stops advertising the summary prefix, the routing table entry is removed.

Examples

The following example redistributes Routing Information Protocol (RIP) routes into IS-IS. In the RIP routing table, there are IPv6 routes for 3FFE:F000:0001:0000::/64, 3FFE:F000:0002:0000::/64, 3FFE:F000:0003:0000::/64, and so on. This example advertises only 3FFE:F000::/24 into IPv6 IS-IS Level 1.

```
Router(config)# router isis area01
Router(config-router)# address-family ipv6
Router(config-router-af)# redistribute rip level-1 metric 40
Router(config-router-af)# summary-prefix 3FFE:F000::/24 level-1
```

summary-prefix (OSPFv3)

To configure an IPv6 summary prefix in Open Shortest Path First version 3 (OSPFv3), use the **summary-prefix** command in OSPFv3 router configuration mode, IPv6 address family configuration mode, or IPv4 address family configuration mode. To restore the default, use the **no** form of this command.

summary-prefix *prefix* [**not-advertise** | **tag** *tag-value*]

no summary-prefix *prefix* [**not-advertise** | **tag** *tag-value*]

Syntax Description

prefix	IPv6 route prefix for the destination.
not-advertise	(Optional) Suppress routes that match the specified prefix and mask pair. This keyword applies to OSPFv3 only.
tag *tag-value*	(Optional) Tag value that can be used as a "match" value for controlling redistribution via route maps. This keyword applies to OSPFv3 only.

Command Default

No IPv6 summary prefix is defined.

Command Modes

OSPFv3 router configuration mode (config-router)
IPv6 address family configuration (config-router-af)
IPv4 address family configuration (config-router-af)

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)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.
15.1(3)S	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.
Cisco IOS XE Release 3.4S	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.
15.2(1)T	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.

Usage Guidelines

This command can be used to summarize routers redistributed from other routing protocols. Multiple groups of addresses can be summarized. The metric used to advertise the summary is the smallest metric of all the more specific routes. This command helps reduce the size of the routing table.

Examples

In the following example, tthe summary prefix FEC0::/24 includes addresses FEC0::/1 through FEC0::/24. Only the address FEC0::/24 is advertised in an external link-state advertisement.

```
summary-prefix FEC0::/24
```

Related Commands

router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

switchport

Cisco 3550, 4000, and 4500 Series Switches

To put an interface that is in Layer 3 mode into Layer 2 mode for Layer 2 configuration, use the **switchport** command in interface configuration mode. To put an interface into Layer 3 mode, use the **no** form of this command.

switchport

no switchport

Cisco Catalyst 6500/6000 Series Switches and Cisco 7600 Series Routers

To modify the switching characteristics of the Layer 2-switched interface, use the **switchport** command (without keywords). Use the **no** form of this command (without keywords) to return the interface to the routed-interface status and cause all further Layer 2 configuration to be erased. Use the **switchport** commands (with keywords) to configure the switching characteristics.

switchport

switchport {**host** | **nonegotiate**}

no switchport

no switchport nonegotiate

Syntax Description

Cisco 3550, 4000, and 4500 Series Switches

This command has no arguments or keywords.

Cisco Catalyst 6500/6000 Series Switches and Cisco 7600 Series Routers

host	Optimizes the port configuration for a host connection.
nonegotiate	Specifies that the device will not engage in negotiation protocol on this interface.

Defaults

Cisco 3550, 4000, and 4500 Series Switches

All interfaces are in Layer 2 mode.

Catalyst 6500/6000 Series Switches and 7600 Series Routers

The default access VLAN and trunk-interface native VLAN are default VLANs that correspond to the platform or interface hardware.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.

Release	Modification
12.2(15)ZJ	This command was implemented on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
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.
15.1(2)T	Support for IPv6 was added.

Usage Guidelines

Cisco 3550, 4000, and 4500 Series Switches

Use the **no switchport** command to put the interface into the routed-interface status and to erase all Layer 2 configurations. You must use this command before assigning an IP address to a routed port. Entering the **no switchport** command shuts down the port and then reenables it, which might generate messages on the device to which the port is connected.

You can verify the switchport status of an interface by entering the **show running-config** privileged EXEC command.

Cisco Catalyst 6500/6000 Series Switches and Cisco 7600 Series Routers

You must enter the **switchport** command without any keywords to configure the LAN interface as a Layer 2 interface before you can enter additional **switchport** commands with keywords. This action is required only if you have not entered the **switchport** command for the interface.

Entering the **no switchport** command shuts down the port and then reenables it. This action may generate messages on the device to which the port is connected.

To optimize the port configuration, entering the **switchport host** command sets the switch port mode to access, enables spanning tree PortFast, and disables channel grouping. Only an end station can accept this configuration.

Because spanning-tree PortFast is enabled, you should enter the **switchport host** command only on ports that are connected to a single host. Connecting other Cisco 7600 series routers, hubs, concentrators, switches, and bridges to a fast-start port can cause temporary spanning-tree loops.

Enable the **switchport host** command to decrease the time that it takes to start up packet forwarding.

The **no** form of the **switchport nonegotiate** command removes **nonegotiate** status.

When using the **nonegotiate** keyword, Dynamic Inter-Switch Link Protocol and Dynamic Trunking Protocol (DISL/DTP)-negotiation packets are not sent on the interface. The device trunks or does not trunk according to the **mode** parameter given: **access** or **trunk**. This command returns an error if you attempt to execute it in **dynamic** (**auto** or **desirable**) mode.

You must force a port to trunk before you can configure it as a SPAN-destination port. Use the **switchport nonegotiate** command to force the port to trunk.

Examples

Cisco 3550, 4000, and 4500 Series Switches

The following example shows how to cause an interface to cease operating as a Layer 2 port and become a Cisco-routed (Layer 3) port:

```
Router(config-if)# no switchport
```

Cisco Catalyst 6500/6000 Series Switches and Cisco 7600 Series Routers

The following example shows how to cause the port interface to stop operating as a Cisco-routed port and convert to a Layer 2-switched interface:

```
Router(config-if)# switchport
Router(config-if)#
```

Note The **switchport** command is not used on platforms that do not support Cisco-routed ports. All physical ports on such platforms are assumed to be Layer 2-switched interfaces.

The following example shows how to optimize the port configuration for a host connection:

```
Router(config-if)# switchport host

switchport mode will be set to access
spanning-tree portfast will be enabled
channel group will be disabled
Router(config-if)#
```

This example shows how to cause a port interface that has already been configured as a switched interface to refrain from negotiating trunking mode and act as a trunk or access port (depending on the **mode** set):

```
Router(config-if)# switchport nonegotiate
Router(config-if)#
```

The following example shows how to cause an interface to cease operating as a Cisco-routed port and to convert it into a Layer 2 switched interface:

```
Router(config-if)# switchport
```

Note The **switchport** command is not used on platforms that do not support Cisco-routed (Layer 3) ports. All physical ports on such platforms are assumed to be Layer 2 switched interfaces.

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings.
show running-config	Displays the current operating configuration.
switchport mode	Sets the interface type.
switchport trunk	Sets trunk characteristics when the interface is in trunking mode.

switchport access vlan

To set the VLAN when the interface is in access mode, use the **switchport access vlan** command in interface configuration mode. To reset the access-mode VLAN to the appropriate default VLAN for the device, use the **no** form of this command.

switchport access vlan *vlan-id*

no switchport access vlan

Syntax Description

vlan-id	VLAN to set when the interface is in access mode; valid values are from 1 to 4094.

Defaults

The defaults are as follows:

- Access VLAN and trunk-interface native VLAN are default VLANs that correspond to the platform or interface hardware.
- All VLAN lists include all VLANs.

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 12.2(33)SRA.

Usage Guidelines

You must enter the **switchport** command without any keywords to configure the LAN interface as a Layer 2 interface before you can enter the **switchport access vlan** command. This action is required only if you have not entered the **switchport** command for the interface.

Entering the **no switchport** command shuts down the port and then reenables it. This action may generate messages on the device to which the port is connected.

The **no** form of the **switchport access vlan** command resets the access-mode VLAN to the appropriate default VLAN for the device.

Examples

This example shows how to cause the port interface to stop operating as a Cisco-routed port and convert to a Layer 2 switched interface:

```
Router(config-if)# switchport
```

Note The **switchport** command is not used on platforms that do not support Cisco-routed ports. All physical ports on such platforms are assumed to be Layer 2-switched interfaces.

This example shows how to cause a port interface that has already been configured as a switched interface to operate in VLAN 2 instead of the platform's default VLAN in the interface-configuration mode:

```
Router(config-if)# switchport access vlan 2
```

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port.
switchport	Configures a LAN interface as a Layer 2 interface.

switchport mode

To set the interface type, use the **switchport mode** command in interface configuration mode. Use the appropriate **no** form of this command to reset the mode to the appropriate default mode for the device.

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

switchport mode {**access** | **trunk**}

no switchport mode

Cisco Catalyst 6500/6000 Series Switches

switchport mode {**access** | **dot1q-tunnel** | **dynamic** {**auto** | **desirable**} | **trunk**}

no switchport mode

Cisco 7600 Series Routers

switchport mode {**access** | **dot1q-tunnel** | **dynamic** {**auto** | **desirable**} | **private-vlan** | **trunk**}

no switchport mode

switchport mode private-vlan {**host** | **promiscuous**}

no switchport mode private-vlan

Syntax Description

access	Sets a nontrunking, nontagged single VLAN Layer 2 interface.
trunk	Specifies a trunking VLAN Layer 2 interface.
dot1q-tunnel	Sets the trunking mode to TUNNEL unconditionally.
dynamic auto	Sets the interface to convert the link to a trunk link.
dynamic desirable	Sets the interface to actively attempt to convert the link to a trunk link.
private-vlan host	Specifies that the ports with a valid private VLAN (PVLAN) association become active host private VLAN ports.
private-vlan promiscuous	Specifies that the ports with a valid PVLAN mapping become active promiscuous ports.

Defaults

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

The default is **access** mode.

Cisco Catalyst 6500/6000 Switches

The default mode is dependent on the platform; it should be either **dynamic auto** for platforms that are intended as wiring closets or **dynamic desirable** for platforms that are intended as backbone switches. The default for PVLAN ports is that no mode is set.

Cisco 7600 Series Routers

The defaults are as follows:

- The mode is dependent on the platform; it should either be **dynamic auto** for platforms that are intended for wiring closets or **dynamic desirable** for platforms that are intended as backbone switches.
- No mode is set for PVLAN ports.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(7)XE	This command was introduced on the Cisco Catalyst 6000 family switches.
12.1(1)E	This command was integrated on the Cisco Catalyst 6000 family switches.
12.1(8a)EX	The switchport mode **private-vlan** {**host** | **promiscuous**} syntax was added.
12.2(2)XT	Creation of switchports became available on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T for creation of switchports on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
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.

Usage Guidelines

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

If you enter a forced mode, the interface does not negotiate the link to the neighboring interface. Ensure that the interface ends match.

The **no** form of the command is not supported on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

Cisco Catalyst 6500/6000 Switches and Cisco 7600 Series Routers

If you enter **access** mode, the interface goes into permanent nontrunking mode and negotiates to convert the link into a nontrunk link even if the neighboring interface does not agree to the change.

If you enter **trunk** mode, the interface goes into permanent trunking mode and negotiates to convert the link into a trunk link even if the neighboring interface does not agree to the change.

If you enter **dynamic auto** mode, the interface converts the link to a trunk link if the neighboring interface is set to **trunk** or **desirable** mode.

If you enter **dynamic desirable** mode, the interface becomes a trunk interface if the neighboring interface is set to **trunk**, **desirable**, or **auto** mode.

If you configure a port as a promiscuous or host-PVLAN port and one of the following applies, the port becomes inactive:

- The port does not have a valid PVLAN association or mapping configured.
- The port is a SPAN destination.

If you delete a private-port PVLAN association or mapping, or if you configure a private port as a SPAN destination, the deleted private-port PVLAN association or mapping or the private port that is configured as a SPAN destination becomes inactive.

If you enter **dot1q-tunnel** mode, PortFast Bridge Protocol Data Unit (BPDU) filtering is enabled and Cisco Discovery Protocol (CDP) is disabled on protocol-tunneled interfaces.

Examples

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

The following example shows how to set the interface to **access** desirable mode:

```
Router(config-if)# switchport mode access
```

The following example shows how to set the interface to **trunk** mode:

```
Router(config-if)# switchport mode trunk
```

Cisco Catalyst 6500/6000 Switches and Cisco 7600 Series Routers

The following example shows how to set the interface to dynamic desirable mode:

```
Router(config-if)# switchport mode dynamic desirable
Router(config-if)#
```

The following example shows how to set a port to PVLAN-host mode:

```
Router(config-if)# switchport mode private-vlan host
Router(config-if)#
```

The following example shows how to set a port to PVLAN-promiscuous mode:

```
Router(config-if)# switchport mode private-vlan promiscuous
Router(config-if)#
```

Related Commands

Command	Description
show dot1q-tunnel	Displays a list of 802.1Q tunnel-enabled ports.
show interfaces switchport	Displays administrative and operational status of a switching (nonrouting) port.
show interfaces trunk	Displays trunk information.
switchport	Modifies the switching characteristics of the Layer 2-switched interface.
switchport private-vlan host-association	Defines a PVLAN association for an isolated or community port.
switchport private-vlan mapping	Defines the PVLAN mapping for a promiscuous port.
switchport trunk	Sets trunk characteristics when the interface is in trunking mode.

synchronization (IPv6)

To enable the synchronization between IPv6 Border Gateway Protocol (BGP) and your Interior Gateway Protocol (IGP) system, use the **synchronization** command in address family configuration mode. To enable the Cisco IOS software to advertise a network route without waiting for IGP, use the **no** form of this command.

synchronization

no synchronization

Syntax Description

This command has no arguments or keywords.

Command Default

BGP advertises network routes without waiting for IGP.

Command Modes

Address family configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
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 Release 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.

Usage Guidelines

Unlike the IPv4 version of the **synchronization** command, the IPv6 version is disabled by default.

By default, an IPv6 BGP speaker advertises an IPv6 network route without waiting for the IGP. Use the **synchronization** command in address family configuration mode to synchronize routing advertisements between BGP and your IGP. This feature allows routers and access servers within an autonomous system to have the route before BGP makes it available to other autonomous systems. When synchronization is enabled, IPv6 BGP does not advertise a route to an external neighbor unless that route is local or exists in the IGP.

Use the **synchronization** command if routers in the autonomous system do not speak BGP.

Examples

The following example enables a router to advertise an IPv6 network route without waiting for an IGP:

```
router bgp 65000
address-family ipv6
 synchronization
```

tacacs server

To configure the TACACS+ server for IPv6 or IPv4 and enter TACACS+ server configuration mode, use the **tacacs server** command in global configuration mode. To remove the configuration, use the **no** form of this command.

tacacs server *name*

no tacacs server

Syntax Description

name	Name of the private TACACS+ server host.

Command Default

No TACACS+ server is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines

The **tacacs server** command configures the TACACS server using the *name* argument and enters TACACS+ server configuration mode. The configuration is applied once you have finished configuration and exited TACACS+ server configuration mode.

Examples

The following example shows how to configure the TACACS server using the name server1 and enter TACACS+ server configuration mode to perform further configuration:

```
Router(config)# tacacs server server1
Router(config-server-tacacs)#
```

Related Commands

Command	Description
address ipv6 (TACACS+)	Configures the IPv6 address of the TACACS+ server.
key (TACACS+)	Configures the per-server encryption key on the TACACS+ server.
port (TACACS+)	Specifies the TCP port to be used for TACACS+ connections.
send-nat-address (TACACS+)	Sends a client's post-NAT address to the TACACS+ server.
single-connection (TACACS+)	Enables all TACACS packets to be sent to the same server using a single TCP connection.
timeout (TACACS+)	Configures the time to wait for a reply from the specified TACACS server.

telnet

To log in to a host that supports Telnet, use the **telnet** command in user EXEC or privileged EXEC mode.

telnet *host* [*port*] [*keyword*]

Syntax Description

host	A hostname or an IP address.
port	(Optional) A decimal TCP port number, or port name; the default is the Telnet router port (decimal 23) on the host.
keyword	(Optional) One of the keywords listed in Table 328.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.0(21)ST	The **/ipv4** and **/ipv6** keywords were added.
12.1	The **/quiet** keyword was added.
12.2(2)T	The **/ipv4** and **/ipv6** keywords were added.
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 Release 12.2(14)S.
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.
12.2(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

Table 328 lists the optional **telnet** command keywords.

Table 328 telnet Keyword Options

Option	Description
/debug	Enables Telnet debugging mode.
/encrypt kerberos	Enables an encrypted Telnet session. This keyword is available only if you have the Kerberized Telnet subsystem. If you authenticate using Kerberos Credentials, the use of this keyword initiates an encryption negotiation with the remote server. If the encryption negotiation fails, the Telnet connection will be reset. If the encryption negotiation is successful, the Telnet connection will be established, and the Telnet session will continue in encrypted mode (all Telnet traffic for the session will be encrypted).

Table 328 telnet Keyword Options (continued)

Option	Description
/ipv4	Specifies version 4 of the IP protocol. If a version of the IP protocol is not specified in a network that supports both the IPv4 and IPv6 protocol stacks, IPv6 is attempted first and is followed by IPv4.
/ipv6	Specifies version 6 of the IP protocol. If a version of the IP protocol is not specified in a network that supports both the IPv4 and IPv6 protocol stacks, IPv6 is attempted first and is followed by IPv4.
/line	Enables Telnet line mode. In this mode, the Cisco IOS software sends no data to the host until you press the **Enter** key. You can edit the line using the standard Cisco IOS software command-editing characters. The **/line** keyword is a local switch; the remote router is not notified of the mode change.
/noecho	Disables local echo.
/quiet	Prevents onscreen display of all messages from the Cisco IOS software.
/route: *path*	Specifies loose source routing. The *path* argument is a list of hostnames or IP addresses that specify network nodes and ends with the final destination.
/source-interface	Specifies the source interface.
/stream	Turns on *stream* processing, which enables a raw TCP stream with no Telnet control sequences. A stream connection does not process Telnet options and can be appropriate for connections to ports running UNIX-to-UNIX Copy Program (UUCP) and other non-Telnet protocols.
port-number	Port number.
bgp	Border Gateway Protocol.
chargen	Character generator.
cmd *rcmd*	Remote commands.
daytime	Daytime.
discard	Discard.
domain	Domain Name Service.
echo	Echo.
exec	EXEC.
finger	Finger.
ftp	File Transfer Protocol.
ftp-data	FTP data connections (used infrequently).
gopher	Gopher.
hostname	Hostname server.
ident	Ident Protocol.
irc	Internet Relay Chat.
klogin	Kerberos login.
kshell	Kerberos shell.
login	Login (rlogin).
lpd	Printer service.

Table 328 telnet Keyword Options (continued)

Option	Description
nntp	Network News Transport Protocol.
pim-auto-rp	Protocol Independent Multicast (PIM) auto-rendezvous point (RP).
node	Connect to a specific Local-Area Transport (LAT) node.
pop2	Post Office Protocol v2.
pop3	Post Office Protocol v3.
port	Destination local-area transport (LAT) port name.
smtp	Simple Mail Transfer Protocol.
sunrpc	Sun Remote Procedure Call.
syslog	Syslog.
tacacs	Specifies TACACS security.
talk	Talk (517).
telnet	Telnet (23).
time	Time (37).
uucp	UNIX-to-UNIX Copy Program (540).
whois	Nickname (43).
www	World Wide Web (HTTP, 80).

With the Cisco IOS implementation of TCP/IP, you are not required to enter the **connect** or **telnet** command to establish a terminal connection. You can enter only the learned hostname—as long as the following conditions are met:

- The hostname is different from a command word for the router.
- The preferred transport protocol is set to **telnet**.

To display a list of the available hosts, use the **show hosts** command. To display the status of all TCP connections, use the **show tcp** command.

The Cisco IOS software assigns a logical name to each connection, and several commands use these names to identify connections. The logical name is the same as the hostname, unless that name is already in use, or you change the connection name with the **name-connection** EXEC command. If the name is already in use, the Cisco IOS software assigns a null name to the connection.

The Telnet software supports special Telnet commands in the form of Telnet sequences that map generic terminal control functions to operating system-specific functions. To issue a special Telnet command, enter the escape sequence and then a command character. The default escape sequence is Ctrl-^ (press and hold the Ctrl and Shift keys and the 6 key). You can enter the command character as you hold down Ctrl or with Ctrl released; you can use either uppercase or lowercase letters. Table 329 lists the special Telnet escape sequences.

Table 329 Special Telnet Escape Sequences

Escape Sequence[1]	Purpose
Ctrl-^ b	Break
Ctrl-^ c	Interrupt Process (IP and IPv6)

Table 329 Special Telnet Escape Sequences

Escape Sequence[1]	Purpose
Ctrl-^ h	Erase Character (EC)
Ctrl-^ o	Abort Output (AO)
Ctrl-^ t	Are You There? (AYT)
Ctrl-^ u	Erase Line (EL)

1. The caret (^) symbol refers to Shift-6 on your keyboard.

At any time during an active Telnet session, you can list the Telnet commands by pressing the escape sequence keys followed by a question mark at the system prompt:

Ctrl-^ ?

A sample of this list follows. In this sample output, the first caret (^) symbol represents the Ctrl key, and the second caret represents Shift-6 on your keyboard:

```
router> ^^?
[Special telnet escape help]
^^B  sends telnet BREAK
^^C  sends telnet IP
^^H  sends telnet EC
^^O  sends telnet AO
^^T  sends telnet AYT
^^U  sends telnet EL
```

You can have several concurrent Telnet sessions open and switch among them. To open a subsequent session, first suspend the current connection by pressing the escape sequence (Ctrl-Shift-6 then x [Ctrl^x] by default) to return to the system command prompt. Then open a new connection with the **telnet** command.

To terminate an active Telnet session, enter any of the following commands at the prompt of the device to which you are connecting:

- **close**
- **disconnect**
- **exit**
- **logout**
- **quit**

Examples

The following example establishes an encrypted Telnet session from a router to a remote host named host1:

```
router> telnet host1 /encrypt kerberos
```

The following example routes packets from the source system host1 to example.com, then to 10.1.0.11, and finally back to *host1*:

```
router> telnet host1 /route:example.com 10.1.0.11 host1
```

The following example connects to a host with the logical name host1:

```
router> host1
```

The following example suppresses all onscreen messages from the Cisco IOS software during login and logout:

```
router> telnet host2 /quiet
```

The following example shows the limited messages displayed when connection is made using the optional **/quiet** keyword:

```
login:User2
Password:
         Welcome to OpenVMS VAX version V6.1 on node CRAW
     Last interactive login on Tuesday, 15-DEC-1998 11:01
     Last non-interactive login on Sunday,  3-JAN-1999 22:32

Server3)logout
    User2        logged out at  16-FEB-2000 09:38:27.85
```

Related Commands

Command	Description
connect	Logs in to a host that supports Telnet, rlogin, or LAT.
kerberos clients mandatory	Causes the **rsh**, **rcp**, **rlogin**, and **telnet** commands to fail if they cannot negotiate the Kerberos Protocol with the remote server.
name connection	Assigns a logical name to a connection.
rlogin	Logs in to a UNIX host using rlogin.
show hosts	Displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses.
show tcp	Displays the status of TCP connections.

timeout (TACACS+)

To configure the time to wait for a reply from the specified TACACS server, use the **timeout** command in TACACS+ server configuration mode. To return to the command default, use the **no** form of this command.

timeout *seconds*

no timeout *seconds*

Syntax Description

seconds	(Optional) Amount of time, in seconds.

Command Default

Time to wait is 5 seconds.

Command Modes

TACACS+ server configuration (config-server-tacacs)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines

Use the **timeout** command to set the time, in seconds, to wait for a reply from the TACACS server. If the **timeout** command is configured, the specified number of seconds overrides the default time of 5 seconds.

Examples

The following example shows how to configure the wait time to 10 seconds:

```
Router(config)# tacacs server server1
Router(config-server-tacacs)# timeout 10
```

Related Commands

Command	Description
tacacs server	Configures the TACACS+ server for IPv6 or IPv4 and enters TACACS server configuration mode.

timers (IPv6 RIP)

To configure update, timeout, hold-down, and garbage-collection timers for an IPv6 RIP routing process, use the **timers** command in router configuration mode. To return the timers to their default values, use the **no** form of this command.

timers *update timeout holddown garbage-collection*

no timers

Syntax Description

update	Interval of time (in seconds) at which updates are sent. This is the fundamental timing parameter of the routing protocol.
timeout	Interval of time (in seconds) after which a route is declared invalid; it should be at least three times the value of the *update* argument. A route becomes invalid when there is an absence of updates that refresh the route. The route then enters a hold-down state. The route is marked inaccessible and advertised as unreachable. However, the route is still used for forwarding packets.
holddown	Interval (in seconds) during which routing information regarding better paths is suppressed. A route enters a hold-down state when it becomes unreachable and the hold-down timer is a value other than zero. (A learned RIP route becomes unreachable when the route is not refreshed or the route is advertised with a metric of 16.) While in hold-down state, the system ignores any new information about the route from RIP or from any protocols that have a worse administrative distance than RIP. A route with a better administrative distance will replace the unreachable route, even if the route is still in a hold-down state.
garbage-collection	Amount of time (in seconds) that must pass from when a route becomes invalid until the route is removed from the routing table.

Command Default

Update timer: 30 seconds
Timeout timer: 180 seconds
Hold-down timer: 0 seconds
Garbage-collection timer: 120 seconds

Command Modes

Router configuration

Command History

Release	Modification
12.2(2)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, and the hold-down timer default value was changed to 0 seconds.
12.2(13)T	The hold-down timer default value was changed to 0 seconds.
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.
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.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **timers** (IPv6 RIP) command is similar to the **timers basic** (RIP) command, except that it is IPv6-specific.

Use the *update* argument to set the time interval between RIP routing updates. If no route update is received for the time interval specified by the *timeout* argument, the route is considered unreachable. Use the *holddown* argument to set a time delay between the route becoming unreachable and the route being considered invalid in the routing table. The use of a hold-down interval is not recommended for RIP because it can introduce long delays in convergence. Use the *garbage-collection* argument to specify the time interval between a route being considered invalid and the route being purged from the routing table.

The basic timing parameters for IPv6 RIP are adjustable. Because IPv6 RIP is executing a distributed, asynchronous routing algorithm, it is important that these timers be the same for all routers and access servers in the network.

Note The current and default timer values are displayed in the output of the **show ipv6 rip** EXEC command. The relationships of the various timers should be preserved, as described previously.

Examples

The following example sets updates to be broadcast every 5 seconds. If a route is not heard from in 15 seconds, the route is declared unusable. Further information is suppressed for an additional 10 seconds. Assuming no updates, the route is flushed from the routing table 20 seconds after the end of the hold-down period.

```
Router(config)# ipv6 router rip cisco
Router(config-rtr)# timers 5 15 10 30
```

Caution By setting a short update period, you run the risk of congesting slow-speed serial lines. Also, if you have many routes in your updates, you can cause the routers to spend an excessive amount of time processing updates.

Related Commands

Command	Description
show ipv6 rip	Displays information about current IPv6 RIP processes.

timers active-time

To adjust Enhanced Interior Gateway Routing Protocol (EIGRP) routing wait time, use the **timers active-time** command in router configuration mode or address-family topology configuration mode. To disable this function, use the **no** form of the command.

timers active-time [*time-limit* | **disabled**]

no timers active-time

Syntax Description

time-limit	(Optional) EIGRP active-time limit (in minutes). Valid range is 1 to 65535.
disabled	(Optional) Disables the timers and permits the routing wait time to remain active indefinitely.

Command Default

This command is disabled by default.

Command Modes

Router configuration (config-router)
Address-family topology configuration (config-router-af-topology)

Command History

Release	Modification
10.0	This command was introduced.
12.4(6)T	Support for IPv6 was added.
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.
15.0(1)M	This command was modified. Address-family topology configuration mode was added. You must enter this command in address-family topology configuration mode for EIGRP named configurations.
12.2(33)SRE	This command was modified. Address-family topology configuration mode was added. You must enter this command in address-family topology configuration mode for EIGRP named configurations.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

In EIGRP, there are timers that control the time that the router waits (after sending a query) before declaring the route to be in the stuck in active (SIA) state.

Examples

In the following example, the routing wait time is 200 minutes on the specified route:

```
Router(config)# router eigrp 5
Router(config-router)# timers active-time 200
```

In the following example, the routing wait time is 200 minutes on the specified address-family route:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# network 10.0.0.0
Router(config-router-af)# topology base
Router(config-router-af-topology)# timers active-time 200
```

In the following example, the routing wait time is indefinite if a route becomes active:

```
Router(config)# router eigrp 5
Router(config-router)# timers active-time disabled
```

In the following example, the routing wait time is indefinite on the specified address-family route:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# network 10.0.0.0
Router(config-router-af)# topology base
Router(config-router-af-topology)# timers active-time disabled
```

In the following example, the routing wait time is 100 minutes on the specified route:

```
Router(config)# ipv6 router eigrp 1
Router(config-router)# timers active-time 100
```

In the following example, the routing wait time is 100 minutes on the specified address-family route:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv6 autonomous-system 4453
Router(config-router-af)# topology base
Router(config-router-af-topology)# timers active-time disabled
```

Related Commands

Command	Description
address-family (EIGRP)	Enters address-family configuration mode to configure an EIGRP routing instance.
ipv6 router eigrp	Configures the EIGRP IPv6 routing process.
network (EIGRP)	Specifies the network for an EIGRP routing process.
router eigrp	Configures the EIGRP address-family process.
show ip eigrp topology	Displays the EIGRP topology table.
show ipv6 eigrp topology	Displays the IPv6 EIGRP topology table.
topology (EIGRP)	Configures an EIGRP process to route IP traffic under the specified topology instance and enters address-family topology configuration mode.

timers lsa arrival

To set the minimum interval at which the software accepts the same link-state advertisement (LSA) from Open Shortest Path First version 3 (OSPFv3) neighbors, use the **timers lsa arrival** command in OSPFv3 router configuration mode. To restore the default value, use the **no** form of this command.

timers lsa arrival *milliseconds*

no timers lsa arrival

Syntax Description

milliseconds	Minimum delay in milliseconds that must pass between acceptance of the same LSA arriving from neighbors. The range is from 0 to 600,000 milliseconds. The default is 1000 milliseconds.

Defaults

1000 milliseconds

Command Modes

OSPFv3 router configuration (config-router)

Command History

Release	Modification
12.0(25)S	This command was introduced.
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.
12.2(33)SRC	Support for IPv6 was added.
12.2(33)SB	Support for IPv6 was added.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.0(1)M	This command was integrated into Cisco IOS Release 12.5(1)M.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.
15.1(3)S	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.
Cisco IOS XE Release 3.4S	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.
15.2(1)T	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.

Usage Guidelines

The **timers lsa arrival** command controls the minimum interval for accepting the same LSA. The "same LSA" is defined as an LSA instance that contains the same LSA ID number, LSA type, and advertising router ID. If an instance of the same LSA arrives sooner than the interval that is set, the LSA is dropped.

We suggest you keep the *milliseconds* value of the **timers lsa arrival** command less than or equal to the neighbors' *hold-interval* value of the **timers throttle lsa all** command.

Examples

The following example sets the minimum interval for accepting the same LSA at 2000 milliseconds:

```
router ospfv3 1
 log-adjacency-changes
 timers throttle lsa all 200 10000 45000
 timers lsa arrival 2000
 network 10.10.4.0 0.0.0.255 area 24
 network 10.10.24.0 0.0.0.255 area 24
```

Related Commands

Command	Description
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.
timers throttle lsa	Sets rate-limiting values for OSPFv3 LSA generation.
timers throttle lsa all	Sets rate-limiting values for LSAs being generated.

timers pacing flood (OSPFv3)

To configure link-state advertisement (LSA) flood packet pacing, use the **timers pacing flood** command in Open Shortest Path First version 3 (OSPFv3) router configuration mode. To restore the default flood packet pacing value, use the **no** form of this command.

timers pacing flood *milliseconds*

no timers pacing flood

Syntax Description

milliseconds	Time (in milliseconds) at which LSAs in the flooding queue are paced in between updates. The configurable range is from 5 milliseconds to 100 milliseconds. The default value is 33 milliseconds.

Command Default

The default is 33 milliseconds.

Command Modes

OSPFv3 router configuration (config-router)

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.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.0(1)M	This command was integrated into Cisco IOS Release 12.5(1)M.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.
15.1(3)S	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.
Cisco IOS XE Release 3.4S	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.
15.2(1)T	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.

Usage Guidelines

Configuring Open Shortest Path First version 3 (OSPF) flood pacing timers allows you to control interpacket spacing between consecutive link-state update packets in the OSPFv3 transmission queue. This command allows you to control the rate at which LSA updates occur to reduce the high CPU or buffer utilization that can occur when an area is flooded with a very large number of LSAs.

The default settings for OSPFv3 packet pacing timers are suitable for the majority of OSPFv3 deployments. Do not change the packet pacing timers unless all other options to meet OSPFv3 packet flooding requirements have been exhausted. Specifically, network operators should prefer

summarization, stub area usage, queue tuning, and buffer tuning before changing the default flood timers. Furthermore, there are no guidelines for changing timer values; each OSPFv3 deployment is unique and should be considered on a case-by-case basis.

Note The network operator assumes risks associated with changing the default flood timer values.

Examples

The following example configures LSA flood packet-pacing updates to occur in 20-millisecond intervals for OSPFv3 routing process 1:

```
Router(config)# router ospfv3 1
Router(config-router)# timers pacing flood 20
```

Related Commands

Command	Description
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.
show ipv6 ospf	Displays general information about OSPF for IPv6 routing processes.
timers pacing lsa-group	Changes the interval at which OSPF LSAs are collected into a group and refreshed, checksummed, or aged.
timers pacing retransmission	Configures LSA retransmission packet pacing.

timers pacing lsa-group (OSPFv3)

To change the interval at which Open Shortest Path First version 3 (OSPFv3) link-state advertisements (LSAs) are collected into a group and refreshed, checksummed, or aged, use the **timers pacing lsa-group** command in router configuration mode. To restore the default value, use the **no** form of this command.

timers pacing lsa-group *seconds*

no timers pacing lsa-group

Syntax Description

seconds	Number of seconds in the interval at which LSAs are grouped and refreshed, checksummed, or aged. The range is from 10 to 1800 seconds. The default value is 240 seconds.

Command Default

The default interval for this command is 240 seconds. OSPFv3 LSA group pacing is enabled by default.

Command Modes

OSPFv3 router configuration (config-router)

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.
15.1(3)S	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.
Cisco IOS XE Release 3.4S	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.
15.2(1)T	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.

Usage Guidelines

This command allows you to control the rate at which LSA updates occur to reduce the high CPU or buffer utilization that can occur when an area is flooded with a very large number of LSAs. The default settings for OSPFv3 packet pacing timers are suitable for the majority of OSPFv3 deployments. Do not change the packet pacing timers unless all other options to meet OSPFv3 packet flooding requirements have been exhausted. Specifically, network operators should prefer summarization, stub area usage, queue tuning, and buffer tuning before changing the default flooding timers. Furthermore, there are no guidelines for changing timer values; each OSPFv3 deployment is unique and should be considered on a case-by-case basis.

Note The network operator assumes the risks associated with changing the default timer values.

Cisco IOS software groups the periodic refresh of LSAs to improve the LSA packing density for the refreshes in large topologies. The group timer controls the interval used for group refreshment of LSAs; however, this timer does not change the frequency that individual LSAs are refreshed (the default refresh rate is every 30 minutes).

The duration of the LSA group pacing is inversely proportional to the number of LSAs the router is handling. For example, if you have about 10,000 LSAs, decreasing the pacing interval would benefit you. If you have a very small database (40 to 100 LSAs), increasing the pacing interval to 10 to 20 minutes might benefit you slightly.

Examples

The following example configures OSPFv3 group packet-pacing updates between LSA groups to occur in 300-second intervals for OSPFv3 routing process 1:

```
Router(config)# router ospfv3 1
Router(config-router)# timers pacing lsa-group 300
```

Related Commands

Command	Description
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.
show ipv6 ospf	Displays general information about OSPF for IPv6 routing processes.
timers pacing flood	Configures LSA flood packet pacing.
timers pacing retransmission	Configures LSA retransmission packet pacing.

timers pacing retransmission (OSPFv3)

To configure link-state advertisement (LSA) retransmission packet pacing in IPv4 Open Shortest Path First version 3 (OSPFv3), use the **timers pacing retransmission** command in OSPFv3 router configuration mode. To restore the default retransmission packet pacing value, use the **no** form of this command.

timers pacing retransmission *milliseconds*

no timers pacing retransmission

Syntax Description

milliseconds	The time (in milliseconds) at which LSAs in the retransmission queue are paced. The configurable range is from 5 milliseconds to 200 milliseconds. The default value is 66 milliseconds.

Command Default

The default is 66 milliseconds.

Command Modes

OSPFv3 router configuration (config-router)

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.
15.1(3)S	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.
Cisco IOS XE Release 3.4S	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.
15.2(1)T	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.

Usage Guidelines

Configuring OSPFv3 retransmission pacing timers allow you to control interpacket spacing between consecutive link-state update packets in the OSPFv3 retransmission queue. This command allows you to control the rate at which LSA updates occur to reduce high CPU or buffer utilization that can occur when an area is flooded with a very large number of LSAs. The default settings for OSPFv3 packet retransmission pacing timers are suitable for the majority of OSPFv3 deployments. Do not change the packet retransmission pacing timers unless all other options to meet OSPFv3 packet flooding requirements have been exhausted. Specifically, network operators should prefer summarization, stub area usage, queue tuning, and buffer tuning before changing the default flooding timers. Furthermore, there are no guidelines for changing timer values; each OSPFv3 deployment is unique and should be considered on a case-by-case basis.

Note The network operator assumes risks associated with changing the default packet retransmission pacing timer values.

Examples

The following example configures LSA flood pacing updates to occur in 100-millisecond intervals for OSPFv3 routing process 1:

```
Router(config)# router ospfv3 1
Router(config-router)# timers pacing retransmission 100
```

Related Commands

Command	Description
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.
show ipv6 ospf	Displays general information about OSPF for IPv6 routing processes.
timers pacing flood	Configures LSA flood packet pacing.
timers pacing lsa-group	Changes the interval at which OSPF LSAs are collected into a group and refreshed, checksummed, or aged.

timers register

To set how long the Session Initiation Protocol (SIP) user agent (UA) waits before sending register requests, use the **timers register** command in SIP user-agent configuration mode. To reset this value to the default, use the **no** form of this command.

timers register *milliseconds*

no timers register

Syntax Description

milliseconds	Waiting time, in milliseconds. Range is from 100 to 1000. Default is 500.

Defaults

500 milliseconds

Command Modes

SIP user-agent configuration

Command History

Release	Modification
12.2(15)ZJ	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4(22)T	Support for IPv6 was added.

Examples

The following example sends register requests every 500 milliseconds:

```
sip-ua
 retry invite 9
 retry register 9
 timers register 500
```

Related Commands

Command	Description
retry register	Sets the total number of SIP registers to send.

timers spf (IPv6)

To turn on Open Shortest Path First (OSPF) for IPv6 shortest path first (SPF) throttling, use the **timers spf** command in router configuration mode. To turn off SPF throttling, use the **no** form of this command.

timers spf *delay holdtime*

no timers spf

Syntax Description

delay	Delay (in milliseconds) in receiving a change in the SPF calculation. The range is from 0 through 4294967295. The default is 5 milliseconds.
holdtime	Hold time (in milliseconds) between consecutive SPF calculations. The range is from 0 through 4294967295. The default is 10 milliseconds.

Command Default

OSPF for IPv6 throttling is always enabled.

Command Modes

Router 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.

Usage Guidelines

The first wait interval between SPF calculations is the amount of time in milliseconds specified by the *delay* argument. Each consecutive wait interval is two times the current hold level in milliseconds until the wait time reaches the maximum time in milliseconds as specified by the *holdtime* argument. Subsequent wait times remain at the maximum until the values are reset or a link-state advertisement (LSA) is received between SPF calculations.

Examples

The following example shows a router configured with the delay and hold-time interval values for the **timers spf** command set at 40 and 50 milliseconds, respectively.

```
Router(config)# ipv6 router ospf 1
Router(config-router)# timers spf 40 50
```

Related Commands

Command	Description
show ipv6 ospf	Displays general information about OSPF for IPv6 routing processes.

timers throttle lsa

To set rate-limiting values for Open Shortest Path First (OSPF) for IPv6 link-state advertisement (LSA) generation, use the **timers throttle lsa** command in router configuration mode. To restore the default values, use the **no** form of this command.

timers throttle lsa *start-interval hold-interval max-interval*

no timers throttle lsa

Syntax Description

start-interval	Minimum delay in milliseconds for the generation of LSAs. The first instance of LSA is always generated immediately upon a local OSPF for IPv6 topology change. The generation of the next LSA is not before the start interval. The range is from 0 to 600,000 milliseconds. The default is 0 milliseconds, which means no delay; the LSA is sent immediately.
hold-interval	Incremental time in milliseconds. This value is used to calculate the subsequent rate limiting times for LSA generation. The range is from 1 to 600,000 milliseconds. The default value is 5000 milliseconds.
max-interval	Maximum wait time in milliseconds between generation of the same LSA. The range is from 1 to 600,000 milliseconds. The default value is 5000 milliseconds.

Defaults

start-interval: 0 milliseconds
hold-interval: 5000 milliseconds
max-interval: 5000 milliseconds

Command Modes

OSPF for IPv6 router configuration (config-rtr)
Router configuration (config-router)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
12.2(33)SB	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.
15.0(1)M	This command was integrated into Cisco IOS Release 12.5(1)M.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

The “same LSA” is defined as an LSA instance that contains the same LSA ID number, LSA type, and advertising router ID. We suggest you keep the *milliseconds* value of the **timers lsa arrival** command less than or equal to the *hold-interval* value of the **timers throttle lsa** command.

Examples

This example customizes OSPF LSA throttling so that the start interval is 200 milliseconds, the hold interval is 10,000 milliseconds, and the maximum interval is 45,000 milliseconds. The minimum interval between instances of receiving the same LSA is 2000 milliseconds.

```
router ospf 1
 log-adjacency-changes
 timers throttle lsa 200 10000 45000
 timers lsa arrival 2000
 network 10.10.4.0 0.0.0.255 area 24
 network 10.10.24.0 0.0.0.255 area 24
```

This example customizes IPv6 OSPF LSA throttling so that the start interval is 500 milliseconds, the hold interval is 1,000 milliseconds, and the maximum interval is 10,000 milliseconds.

```
ipv6 router ospf 1
 log-adjacency-changes
 timers throttle lsa 500 1000 10000
```

Related Commands

Command	Description
show ipv6 ospf	Displays information about OSPF for IPv6 routing processes.
timers lsa arrival	Sets the minimum interval at which the software accepts the same LSA from OSPF neighbors.

timers throttle spf

To turn on Open Shortest Path First (OSPF) shortest path first (SPF) throttling, use the **timers throttle spf** command in the appropriate configuration mode. To turn off OSPF SPF throttling, use the **no** form of this command.

timers throttle spf *spf-start spf-hold spf-max-wait*

no timers throttle spf *spf-start spf-hold spf-max-wait*

Syntax Description

spf-start	Initial delay to schedule an SFP calculation after a change, in milliseconds. Range is from 1 to 600000. In OSPF for IPv6, the default value is 5000.
spf-hold	Minimum hold time between two consecutive SPF calculations, in milliseconds. Range is from 1 to 600000. In OSPF for IPv6, the default value is 10,000.
spf-max-wait	Maximum wait time between two consecutive SPF calculations, in milliseconds. Range is from 1 to 600000. In OSPF for IPv6, the default value is 10,000.

Command Default

SPF throttling is not set.

Command Modes

Address family configuration (config-router-af)
Router address family topology configuration (config-router-af-topology)
Router configuration (config-router)
OSPF for IPv6 router configuration (config-rtr)

Command History

Release	Modification
12.2(14)S	This command was introduced.This command replaces the **timers spf-interval** command.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
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.
12.2(33)SRB	This command was made available in router address family configuration mode.
12.2SX	This command is supported in the Cisco 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	Support for IPv6 was added.
12.2(33)SB	Support for IPv6 was added and this command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Release	Modification
15.0(1)M	This command was integrated into Cisco IOS Release 12.5(1)M.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

The first wait interval between SPF calculations is the amount of time in milliseconds specified by the *spf-start* argument. Each consecutive wait interval is two times the current hold level in milliseconds until the wait time reaches the maximum time in milliseconds as specified by the *spf-max-wait* argument. Subsequent wait times remain at the maximum until the values are reset or a link-state advertisement (LSA) is received between SPF calculations.

Release 12.2(33)SRB

If you plan to configure the Multi-Topology Routing (MTR) feature, you need to enter the **timers throttle spf** command in router address family topology configuration mode in order to make this OSPF router configuration command become topology-aware.

Examples

The following example shows how to configure a router with the delay, hold, and maximum interval values for the **timers throttle spf** command set at 5, 1000, and 90,000 milliseconds, respectively.

```
router ospf 1
 router-id 10.10.10.2
 log-adjacency-changes
 timers throttle spf 5 1000 90000
 redistribute static subnets
 network 10.21.21.0 0.0.0.255 area 0
 network 10.22.22.0 0.0.0.255 area 00
```

The following example shows how to configure a router using IPv6 with the delay, hold, and maximum interval values for the **timers throttle spf** command set at 500, 1000, and 10,000 milliseconds, respectively.

```
ipv6 router ospf 1
 event-log size 10000 one-shot
 log-adjacency-changes
 timers throttle spf 500 1000 10000
```

traceroute

To discover the routes that packets will actually take when traveling to their destination address, use the **traceroute** command in user EXEC or privileged EXEC mode.

traceroute [**vrf** *vrf-name* | **topology** *topology-name*] [*protocol*] *destination*

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name of a Virtual Private Network (VPN) routing and forwarding (VRF) instance table in which to find the destination address. The only keyword that you can select for the *protocol* argument when you use the **vrf** *vrf-name* keyword-argument pair is the **ip** keyword.
topology *topology-name*	(Optional) Specifies the name of the topology instance. The *topology-name* argument is case-sensitive; "VOICE" and "voice" specify different topologies.
protocol	(Optional) Protocol keyword, either **appletalk**, **clns**, **ip**, **ipv6**, **ipx**, **oldvines**, or **vines**. When not specified, the *protocol* argument is based on an examination by the software of the format of the *destination* argument. The default protocol is IP.
destination	(Optional in privileged EXEC mode; required in user EXEC mode) The destination address or hostname for which you want to trace the route. The software determines the default parameters for the appropriate protocol and the tracing action begins.

Command Default

When not specified, the *protocol* argument is determined by the software examining the format of the *destination* argument. For example, if the software finds a *destination* argument in IP format, the protocol value defaults to IP.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.0(5)T	The **vrf** *vrf-name* keyword and argument were added.
12.2(2)T	Support for IPv6 was added.
12.0(21)ST	Support for IPv6 was added.
12.0(22)S	Support for IPv6 was added.
12.2(11)T	The **traceroute** command test characters for IPv6 were updated. A new error message was added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.

Release	Modification
12.3(5)	A line was added to the interactive **traceroute vrf** command, so that you can resolve the autonomous system number through the use of the global table or a VRF table, or you can choose not to resolve the autonomous system.
12.0(26)S1	Changes to the command were integrated into Cisco IOS Release 12.0(26)S1.
12.2(20)S	Changes to the command were integrated into Cisco IOS Release 12.2(20)S.
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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	The **topology** *topology-name* keyword and argument were added to support Multi-Topology Routing (MTR).
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 3.2S	This command was modified. When the **vrf** keyword is used, the output displays the incoming VRF name/tag and the outgoing VRF name/tag.

Usage Guidelines

The **traceroute** command works by taking advantage of the error messages generated by routers when a datagram exceeds its hop limit value.

The **traceroute** command starts by sending probe datagrams with a hop limit of 1. Including a hop limit of 1 with a probe datagram causes the neighboring routers to discard the probe datagram and send back an error message. The **traceroute** command sends several probes with increasing hop limits and displays the round-trip time for each.

The **traceroute** command sends out one probe at a time. Each outgoing packet might result in one or more error messages. A time-exceeded error message indicates that an intermediate router has seen and discarded the probe. A destination unreachable error message indicates that the destination node has received and discarded the probe because the hop limit of the packet reached a value of 0. If the timer goes off before a response comes in, the **traceroute** command prints an asterisk (*).

The **traceroute** command terminates when the destination responds, when the hop limit is exceeded, or when the user interrupts the trace with the escape sequence. By default, to invoke the escape sequence, type **Ctrl-^ X**—by simultaneously pressing and releasing the **Ctrl**, **Shift**, and **6** keys, and then pressing the **X** key.

To use nondefault parameters and invoke an extended **traceroute** test, enter the command without a *protocol* or *destination* argument in privileged EXEC mode. You are stepped through a dialog to select the desired parameters. Extended **traceroute** tests are not supported in user EXEC mode. The user-level traceroute feature provides a basic trace facility for users who do not have system privileges. The *destination* argument is required in user EXEC mode.

If the system cannot map an address for a hostname, it returns a "%No valid source address for destination" message.

If the **vrf** *vrf-name* keyword and argument are used, the **topology** option is not displayed because only the default VRF is supported. The **topology** *topology-name* keyword and argument and the DiffServ Code Point (DSCP) option in the extended traceroute system dialog are displayed only if a topology is configured on the router.

In Cisco IOS XE Release 3.2S, output of the **traceroute** command with the **vrf** keyword was enhanced to make troubleshooting easier by displaying the incoming VRF name/tag and the outgoing VRF name/tag.

Examples

After you enter the **traceroute** command in privileged EXEC mode, the system prompts you for a protocol. The default protocol is IP.

If you enter a hostname or address on the same line as the **traceroute** command, the default action is taken as appropriate for the protocol type of that name or address.

The following example is sample dialog from the **traceroute** command using default values. The specific dialog varies somewhat from protocol to protocol.

```
Router# traceroute

Protocol [ip]:
Target IP address:
Source address:
DSCP Value [0]: ! Only displayed if a topology is configured on the router.
Numeric display [n]:
Timeout in seconds [3]:
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Port Number [33434]:
Loose, Strict, Record, Timestamp, Verbose [none]:
```

The following example displays output available in Cisco IOS XE Release 3.2S and later. Output of the **traceroute** command with the **vrf** keyword includes the incoming VRF name/tag and the outgoing VRF name/tag.

```
Router# traceroute vrf red 10.0.10.12

Type escape sequence to abort.
Tracing the route to 10.0.10.12
VRF info: (vrf in name/id, vrf out name/id)
  1 10.1.13.15 (red/13,red/13) 0 msec
    10.1.16.16 (red/13,red/13) 0 msec
    10.1.13.15 (red/13,red/13) 1 msec
  2 10.1.8.13 (red/13,red/13) 0 msec
    10.1.7.13 (red/13,red/13) 0 msec
    10.1.8.13 (red/13,red/13) 0 msec
  3 10.1.2.11 (red/13,blue/10) 1 msec 0 msec 0 msec
  4  *  *  *
```

Related Commands

Command	Description
ping (MTR)	Pings a destination within a specific topology.

track interface

To configure an interface to be tracked and to enter tracking configuration mode, use the **track interface** command in global configuration mode. To remove the tracking, use the **no** form of this command.

track *object-number* **interface** *type number* {**line-protocol** | **ip routing**}

no track *object-number* **interface** *type number* {**line-protocol** | **ip routing**}

Syntax Description

object-number	Object number that represents the interface to be tracked. The range is from 1 to 1000.
type number	Interface type and number to be tracked. No space is required between the values.
line-protocol	Tracks the state of the interface line protocol.
ip routing	Tracks whether IP routing is enabled, whether an IP address is configured on the interface, and whether the interface state is up before reporting to the tracking client that the interface is up.

Command Default

No interface is tracked.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(11)T	The **track interface ip routing** command was enhanced to allow the tracking of an IP address on an interface that was acquired through DHCP or PPP IPCP.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(18)SXF	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.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.1(3)T	This command was modified. The valid range of the *object-number* argument increased to 1000.
15.1(1)S	This command was modified. The valid range for the *object-number* argument increased to 1000.

Usage Guidelines

This command reports a state value to clients. A tracked IP-routing object is considered up when the following criteria exist:

- IP routing is enabled and active on the interface.
- The interface line-protocol state is up.
- The interface IP address in known. The IP address is configured or received through the Dynamic Host Configuration Protocol (DHCP) or IP Control Protocol (IPCP) negotiation.

Interface IP routing will go down when one of the following criteria exist:

- IP routing is disabled globally.
- The interface line-protocol state is down.
- The interface IP address is unknown. The IP address is not configured or received through DHCP or IPCP negotiation.

No space is required between the *type number* values.

Tracking the IP-routing state of an interface using the **track interface ip routing** command can be more useful in some situations than just tracking the line-protocol state using the **track interface line-protocol** command, especially on interfaces for which IP addresses are negotiated. For example, on a serial interface that uses the Point-to-Point Protocol (PPP), the line protocol could be up (link control protocol [LCP] negotiated successfully), but IP could be down (IPCP negotiation failed).

The **track interface ip routing** command supports the tracking of an interface with an IP address acquired through any of the following methods:

- Conventional IP address configuration
- PPP/IPCP
- DHCP
- Unnumbered interface

As of Cisco IOS Release 15.1(3)T, a maximum of 1000 objects can be tracked. Although 1000 tracked objects can be configured, each tracked object uses CPU resources. The amount of available CPU resources on a router is dependent upon variables such as traffic load and how other protocols are configured and run. The ability to use 1000 tracked objects is dependent upon the available CPU. Testing should be conducted on site to ensure that the service works under the specific site traffic conditions.

Examples

In the following example, the tracking process is configured to track the IP-routing capability of serial interface 1/0:

```
Router(config)# track 1 interface serial1/0 ip routing
Router(config-track)#
```

Related Commands

Command	Description
show track	Displays HSRP tracking information.

tracking

To override the default tracking policy on a port, use the **tracking** command in Neighbor Discovery (ND) inspection policy configuration mode.

tracking {**enable** [**reachable-lifetime** {*value* | **infinite**}] | **disable** [**stale-lifetime** {*value* | **infinite**}]}

Syntax Description

enable	Tracking is enabled.
reachable-lifetime	(Optional) The maximum amount of time a reachable entry is considered to be directly or indirectly reachable without proof of reachability. • The **reachable-lifetime** keyword can be used only with the **enable** keyword. • Use of the **reachable-lifetime** keyword overrides the global reachable lifetime configured by the **ipv6 neighbor binding reachable-lifetime** command.
value	Lifetime value, in seconds. The range is from 1 to 86,400 seconds, and the default is 300 seconds.
infinite	An entry is kept in a reachable or stale state for an infinite amount of time.
disable	Tracking is disabled.
stale-lifetime	(Optional) The time entry is kept in a stale state, which overwrites the global stale-lifetime configuration. • The stale lifetime is 86,400 seconds. • The **stale-lifetime** keyword can be used only with the **disable** keyword. • Use of the **stale-lifetime** keyword overrides the global stale lifetime configured by the **ipv6 neighbor binding stale-lifetime** command.

Command Default

The time entry is kept in a reachable state.

Command Modes

ND inspection policy configuration (config-nd-inspection)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

The **tracking** command overrides the default tracking policy set by the **ipv6 neighbor tracking** command on the port on which this policy applies. This function is useful on trusted ports where, for example, one may not want to track entries but wants an entry to stay in the binding table to prevent it from being stolen.

The **reachable-lifetime** keyword is the maximum time an entry will be considered reachable without proof of reachability, either directly through tracking, or indirectly through ND inspection. After the **reachable-lifetime** value is reached, the entry is moved to stale. Use of the **reachable-lifetime** keyword with the **tracking** command overrides the global reachable lifetime configured by the **ipv6 neighbor binding reachable-lifetime** command.

The **stale-lifetime** keyword is the maximum time an entry is kept in the table before it is deleted or the entry is proven to be reachable, either directly or indirectly. Use of the **stale-lifetime** keyword with the **tracking** command overrides the global stale lifetime configured by the **ipv6 neighbor binding stale-lifetime** command.

Examples

The following example defines an ND policy name as policy1, places the router in ND inspection policy configuration mode, and configures an entry to stay in the binding table for an infinite length of time on a trusted port:

```
Router(config)# ipv6 nd inspection policy policy1
Router(config-nd-inspection)# tracking disable stale-lifetime infinite
```

Related Commands

Command	Description
ipv6 nd inspection policy	Defines the ND inspection policy name and enters ND inspection policy configuration mode.
ipv6 neighbor binding	Changes the defaults of neighbor binding entries in a binding table.
ipv6 neighbor tracking	Enables tracking of entries in the binding table.
ipv6 nd raguard policy	Defines the RA guard policy name and enter RA guard policy configuration mode.

translation-profile (dial peer)

To assign a translation profile to a dial peer, use the **translation-profile** command in dial peer configuration mode. To delete the translation profile from the dial peer, use the **no** form of this command.

translation-profile {**incoming** | **outgoing**} *name*

no translation-profile {**incoming** | **outgoing**} *name*

Syntax Description

incoming	Specifies that this translation profile handles incoming calls.
outgoing	Specifies that this translation profile handles outgoing calls.
name	Name of the translation profile.

Defaults

No default behavior or values

Command Modes

Dial peer configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.
12.4(22)T	Support for IPv6 was added.

Usage Guidelines

Use the **translation-profile** command to assign a predefined translation profile to a dial peer.

Examples

The following example assigns the translation profile named "profile1" to handle translation of outgoing calls for a dial peer:

```
Router(config)# dial-peer voice 111 pots
Router(config-dial-peer)# translation-profile outgoing profile1
```

Related Commands

Command	Description
rule (voice translation-rule)	Sets the criteria for the translation rule.
show voice translation-profile	Displays the configuration of a translation profile.
translate (translation profiles)	Assigns a translation rule to a translation profile.
voice translation-profile	Initiates the translation-profile definition.
voice translation-rule	Initiates the translation-rule definition.

trusted-port (IPv6 ND Inspection Policy)

To configure a port to become a trusted port, use the **trusted-port** command in Neighbor Discovery Protocol (NDP) inspection policy configuration mode. To disable this function, use the **no** form of this command.

trusted-port

no trusted-port

Syntax Description

This command has no arguments or keywords.

Command Default

No ports are trusted.

Command Modes

NDP inspection policy configuration (config-nd-inspection)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

When the **trusted-port** command is enabled, limited or no verification is performed when messages are received on ports that have this policy. However, to protect against address spoofing, messages are analyzed so that the binding information that they carry can be used to maintain the binding table. Bindings discovered from these ports will be considered more trustworthy than bindings received from ports that are not configured to be trusted.

Use the **trusted-port** command after enabling NDP inspection policy configuration mode using the **ipv6 nd inspection policy** command.

Examples

The following example defines an NDP policy name as policy1, places the router in NDP inspection policy configuration mode, and configures the port to be trusted:

```
Router(config)# ipv6 nd inspection policy policy1
Router(config-nd-inspection)# trusted-port
```

Related Commands

Command	Description
ipv6 nd inspection policy	Defines the NDP inspection policy name and enters NDP inspection policy configuration mode.

trusted-port (IPv6 RA Guard Policy)

To configure a port to become a trusted port, use the **trusted-port** command in router advertisement (RA) guard policy configuration. To disable this function, use the **no** form of this command.

trusted-port

no trusted-port

Syntax Description

This command has no arguments or keywords.

Command Default

No ports are trusted.

Command Modes

RA guard policy configuration (config-ra-guard)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

When the **trusted-port** command is enabled, limited or no verification is performed when messages are received on ports that have this policy. However, the **device-role** command takes precedence over the **trusted-port** command; if the device role is configured as host, messages will be dropped regardless of **trusted-port** command configuration.

Examples

The following example defines an RA guard policy name as raguard1, places the router in RA guard policy configuration mode, and configures the port to be trusted:

```
Router(config)# ipv6 nd inspection policy policy1
Router(config-ra-guard)# trusted-port
```

Related Commands

Command	Description
ipv6 nd inspection policy	Defines the NDP inspection policy name and enters NDP inspection policy configuration mode.
ipv6 nd raguard policy	Defines the RA guard policy name and enter RA guard policy configuration mode.

tunnel 6rd br

To bypass security checks on an IPv6 rapid deployment (6RD) customer-edge (CE) router, use the **tunnel 6rd br command** in interface configuration mode. To remove the BR router's address from configuration, use the **no** form of this command.

tunnel 6rd br *ipv4-address*

no tunnel 6rd br *ipv4-address*

Syntax Description

ipv4-address	IPv4 address of the BR router.

Command Default

No BR router is specified.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T.

Usage Guidelines

The **tunnel 6rd br** command is optional for 6RD operation. The command allows the user to specify the BR address, which allows the 6RD router to skip the security checks for packets from that source.

By default at a 6RD router, all incoming packets require that their outer IPv4 source address to be embedded in the 6RD-encoded IPv6 source address. Packets that do not satisfy this criteria are dropped. Configuring the **tunnel 6rd br** command exempts packets with the specified source from this check.

The **tunnel 6rd br** command should be enabled on the customer edge (CE) router, because packets arriving at the CE from the BR typically are traffic from a native IPv6 host, which does not need to have a 6RD-encoded source address.

Examples

The following example sets the BR address to 10.1.4.1:

```
Router(config-if)# tunnel 6rd br 10.1.4.1
```

Related Commands

Command	Description
ip address	Specifies the IPv4 address of an IPv4 interface.
ipv6 address	Configures an IPv6 address based on an IPv6 general prefix and enables IPv6 processing on an interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

Command	Description
tunnel destination	Sets the destination address for a tunnel interface.
tunnel source	Sets the source address for a tunnel interface.

tunnel 6rd ipv4

To specify the prefix length and suffix length of the IPv4 transport address common to all the 6RD routers in a domain, use the **tunnel 6rd ipv4** command in interface configuration mode. To remove these parameters, use the **no** form of this command.

tunnel 6rd ipv4 {**prefix-len** *length*} {**suffix-len** *length*}

no tunnel 6rd ipv4 {**prefix-len** *length*} {**suffix-len** *length*}

Syntax Description

prefix-len *length*	Specifies the prefix length, in bits, common to all 6RD routers in a domain. • The range is from 0 to 31, and the default is 0. • The sum of the IPv4 prefix length and the IPv4 suffix length cannot exceed 31.
suffix-len *length*	Specifies the suffix length, in bits, common to all 6RD routers in a domain. • The range is from 0 to 31, and the default is 0. • The sum of the IPv4 prefix length and the IPv4 suffix length cannot exceed 31.

Command Default

The prefix length and suffix length are 0.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T.

Usage Guidelines

The **tunnel 6rd ipv4** command is optional for 6RD operation. This command specifies the number of most significant bits and least significant bits of the IPv4 transport address (that is, the tunnel source) that are common to all the 6RD routers in a domain. The valid range is from 0 to 31, and the sum of the IPv4 prefix length and the IPv4 suffix length cannot exceed 31. If the **tunnel 6rd ipv4** command is not configured, and the **tunnel 6rd prefix** command is configured, the system uses the default value of 0.

Examples

The following example shows 6RD configuration, including the number of most and least significant bits of the IPv4 transport address common to all the 6RD routers in a domain:

```
Router(config)# interface Tunnel1
Router(config-if)# ipv6 address 2001:B000:100::1/32
Router(config-if)# tunnel source GigabitEthernet2/0/0
Router(config-if)# tunnel mode ipv6ip 6rd
Router(config-if)# tunnel 6rd prefix 2001:B000::/32
```

```
Router(config-if)# tunnel 6rd ipv4 prefix-len 16 suffix-len 8
```

Related Commands

Command	Description
ip address	Specifies the IP address of an IPv4 interface.
ipv6 address	Configures an IPv6 address based on an IPv6 general prefix and enables IPv6 processing on an interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.
tunnel 6rd prefix	Specifies the common IPv6 prefix on 6RD tunnels
tunnel destination	Sets the destination address for a tunnel interface.
tunnel source	Sets the source address for a tunnel interface.

tunnel 6rd prefix

To specify the common IPv6 prefix on IPv6 rapid deployment (6RD) tunnels, use the **tunnel 6rd prefix** command in interface configuration mode. To remove the IPv6 prefix, use the **no** form of this command.

tunnel 6rd prefix *ipv6-prefix*/*prefix-length*

no tunnel 6rd prefix *ipv6-prefix*/*prefix-length*

Syntax Description

ipv6-prefix	The IPv6 network assigned to the general prefix. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/prefix-length	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

Command Default

This command can be enabled only when 6RD is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T.

Usage Guidelines

The **tunnel 6rd prefix** command is mandatory for 6RD operation. It specifies the common IPv6 prefix, and the *prefix-length* argument determines us the position of the IPv4 address in the 6RD delegated prefix (or payload) destination. Configuring a *prefix-length* of 0 is equivalent to removing this command.

The tunnel line state of a 6RD tunnel remains inactive until the **tunnel 6rd prefix** command is configured, and this command is automatically disabled when the **tunnel mode ipv6ip** command is configured to use a keyword other than **6rd**.

Examples

The following example shows 6RD configuration, including the **tunnel 6rd prefix** command:

```
ipv6 general-prefix 6rd1 6rd Tunnel1
!
interface Tunnel1
 ipv6 address 6rd1 ::1/124
tunnel source GigabitEthernet2/0/0
tunnel mode ipv6ip 6rd
tunnel 6rd prefix 2001:B000::/32
tunnel 6rd ipv4 prefix-len 16 suffix-len 8
```

Related Commands

Command	Description
ip address	Specifies the IPv4 address of an IPv4 interface.
ipv6 address	Configures an IPv6 address based on an IPv6 general prefix and enables IPv6 processing on an interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.
tunnel destination	Sets the destination address for a tunnel interface.
tunnel source	Sets the source address for a tunnel interface.

tunnel destination

To specify the destination for a tunnel interface, use the **tunnel destination** command in interface configuration mode. To remove the destination, use the **no** form of this command.

tunnel destination {*host-name* | *ip-address* | *ipv6-address*}

no tunnel destination

Syntax Description

host-name	Name of the host destination.
ip-address	IP address of the host destination expressed in dotted decimal notation.
ipv6-address	IPv6 address of the host destination expressed in IPv6 address format.

Command Default

No tunnel interface destination is specified.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.3(7)T	The address field was modified to accept an *ipv6-address* argument to allow IPv6 nodes to be configured as a tunnel destination.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)S.
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.
12.2(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.

Usage Guidelines

You cannot configure two tunnels to use the same encapsulation mode with exactly the same source and destination address. The workaround is to create a loopback interface and configure the packet source off of the loopback interface. Refer to the *Cisco IOS AppleTalk*, *DECnet*, *ISO CLNS*, *and Novell IPX Configuration Guide* for more information on AppleTalk Cayman tunneling.

Examples

Tunnel Destination Address for Cayman Tunnel Example

The following example shows how to configure the tunnel destination address for Cayman tunneling:

```
Router(config)# interface tunnel0
Router(config-if)# tunnel source ethernet0
```

```
Router(config-if)# tunnel destination 10.108.164.19
Router(config-if)# tunnel mode cayman
```

Tunnel Destination Address for GRE Tunneling Example

The following generic routing encapsulation (GRE) example shows how to configure the tunnel destination address for GRE tunneling:

```
Router(config)# interface tunnel0
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 ip
```

Tunnel Destination Address for IPv6 Tunnel Example

The following GRE example shows how to configure the tunnel destination address for GRE tunneling of IPv6 packets:

```
Router(config)# interface Tunnel0
Router(config-if)#  no ip address
Router(config-if)#  ipv6 router isis
Router(config-if)#  tunnel source Ethernet0/0
Router(config-if)#  tunnel destination 2001:0DB8:1111:2222::1/64
Router(config-if)#  tunnel mode gre ipv6
Router(config-if)# exit
!
Router(config)# interface Ethernet0/0
Router(config-if)#  ip address 10.0.0.1 255.255.255.0
Router(config-if)# exit
!
Router(config)# ipv6 unicast-routing

Router(config)# router isis
Router(config)#  net 49.0000.0000.000a.00
```

Related Commands

Command	Description
appletalk cable-range	Enables an extended AppleTalk network.
appletalk zone	Sets the zone name for the connected AppleTalk network.
tunnel mode	Sets the encapsulation mode for the tunnel interface.
tunnel source	Sets the source address of a tunnel interface.

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.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

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 mode ipv6ip

To configure a static IPv6 tunnel interface, use the **tunnel mode ipv6ip** command in interface configuration mode. To remove an IPv6 tunnel interface, use the **no** form of this command.

tunnel mode ipv6ip [**6rd** | **6to4** | **auto-tunnel** | **isatap**]

no tunnel mode ipv6ip

Syntax Description

6rd	(Optional) Specifies that the tunnel is to be used for IPv6 rapid deployment (6RD).
6to4	(Optional) Specifies IPv6 automatic tunneling mode using a 6to4 address.
auto-tunnel	(Optional) Specifies IPv6 automatic tunneling mode using an IPv4-compatible IPv6 address.
isatap	(Optional) Specifies IPv6 automatic tunneling mode as Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) to connect IPv6 nodes (hosts and routers) within IPv4 networks.

Command Default

IPv6 tunnel interfaces are not configured.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)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	The ISATAP keyword was added to support the addition of ISATAP tunnel implementation.
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.
12.2(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 introduced on Cisco ASR 1000 series routers.
Cisco IOS XE Release 3.1S	The **6rd** keyword was added. The **auto-tunnel** keyword is not supported on Cisco ASR 1000 series routers.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T.

Usage Guidelines

IPv6 tunneling consists of encapsulating IPv6 packets within IPv4 packets for transmission across an IPv4 routing infrastructure.

Manually Configured Tunnels

Using the **tunnel mode ipv6ip** command without keywords specifies an IPv6 configured tunnel where a manually configured IPv6 address is configured on a tunnel interface and manually configured IPv4 addresses are configured as the tunnel source and the tunnel destination. The host or router at each end of an IPv6 configured tunnel must support both the IPv4 and IPv6 protocol stacks.

Automatic Determination of Tunnel Source and Destination

Using the **tunnel mode ipv6ip** command with the **auto-tunnel** keyword specifies an IPv6 automatic tunnel where the tunnel destination is automatically determined by the IPv4 address in the low-order 32 bits of IPv4-compatible IPv6 addresses. An IPv4-compatible IPv6 address is a 128-bit IPv6 address that contains the IPv6 prefix 0:0:0:0:0:0 in the high-order 96 bits of the address and an IPv4 address in the low-order 32 bits of the address. The host or router at each end of an automatic tunnel must support both the IPv4 and IPv6 protocol stacks.

6to4 Tunnels

Using the **tunnel mode ipv6ip** command with the **6to4** keyword specifies automatic 6to4 tunneling where the tunnel endpoint is determined by the globally unique IPv4 address embedded in a 6to4 address. A 6to4 address is a combination of the prefix 2002::/16 and a globally unique 32-bit IPv4 address. (IPv4-compatible addresses are not used in 6to4 tunneling.) The unique IPv4 address is used as the network-layer address in the 6to4 address prefix. The border router at each end of a 6to4 tunnel must support both the IPv4 and IPv6 protocol stacks. The 6to4 tunnel must be configured with the **tunnel source** command to use an interface with an IPv4 address as the source of the tunnel. Additionally, the 6to4 address prefix must be routed over the tunnel using the **ipv6 route** command.

6RD Tunnels

Use the **tunnel mode ipv6ip** command with the **6rd** keyword specifies that the tunnel is to be used for IPv6 RD. The 6RD feature is similar to the 6to4 tunnel feature but it does not require addresses to have a 2002::/16 prefix nor does it require that all the 32 bits of the IPv4 destination be in the IPv6 payload header.

ISATAP Tunnels

ISATAP tunnels enable transport of IPv6 packets within network boundaries. ISATAP tunnels allow individual IPv4/IPv6 dual-stack hosts within a site to connect to an IPv6 network using the IPv4 infrastructure.

Unlike IPv4-compatible addresses, ISATAP IPv6 addresses can use any initial unicast /64 prefix. The final 64 bits are an interface identifier. Of these, the leading 32 bits are the fixed pattern 0000:5EFE; the last 32 bits carry the tunnel endpoint IPv4 address.

Examples

Manually Configured IPv6 Tunnel Example

The following example configures a manual IPv6 tunnel. In the example, tunnel interface 0 is manually configured with a global IPv6 address. The tunnel source and destination are also manually configured.

```
Router(config)# interface tunnel 0
Router(config-if)# ipv6 address 3ffe:b00:c18:1::3/127
Router(config-if)# tunnel source ethernet 0
Router(config-if)# tunnel destination 192.168.30.1
Router(config-if)# tunnel mode ipv6ip
```

IPv4 Compatible IPv6 Address Tunnel Example

The following example configures an automatic IPv6 tunnel that uses Ethernet interface 0 as the tunnel source. The tunnel destination is automatically determined by the IPv4 address in the low-order 32 bits of an IPv4-compatible IPv6 address.

```
Router(config)# interface tunnel 0
Router(config-if)# no ip address
Router(config-if)# tunnel source ethernet 0
Router(config-if)# tunnel mode ipv6ip auto-tunnel
```

6to4 Tunnel Example

The following example configures a 6to4 tunnel. 6to4 tunnels allows for autoconfiguration where a site-specific 48-bit prefix is dynamically constructed by prepending the prefix 2002 to an IPv4 address assigned to the site. In the example, Ethernet interface 0 is configured with an IPv4 address, and with a 64-bit prefix (/64) which is part of the previously constructed 48-bit prefix (/48). Tunnel interface 0 is configured without an IPv4 or IPv6 address because the IPv4 or IPv6 addresses on Ethernet interface 0 is used to construct a tunnel source address. A tunnel destination address is not specified because the destination address is automatically constructed. An IPv6 static route for network 2002::/16 to tunnel interface 0 is configured (traffic destined for the prefix is routed over tunnel interface 0).

```
Router(config)# interface ethernet 0
Router(config-if)# ip address 192.168.99.1 255.255.255.0
Router(config-if)# ipv6 address 2002:c0a8:6301:1::/64 eui-64
Router(config-if)# exit
Router(config)# interface tunnel 0
Router(config-if)# no ip address
Router(config-if)# ipv6 unnumbered ethernet 0
Router(config-if)# tunnel source ethernet 0
Router(config-if)# tunnel mode ipv6ip 6to4
Router(config-if)# exit
Router(config)# ipv6 route 2002::/16 tunnel 0
```

Tunnel Interface Configured with the ipv6 unnumbered Command Example

When a tunnel interface is configured using the **ipv6 unnumbered** command with the **tunnel source** and **tunnel mode ipv6ip** commands, the tunnel uses the first IPv6 address configured on the source interface as its IPv6 address. For 6to4 tunnels, the first IPv6 address configured on the source interface must be a 6to4 address. In the following example, the first IPv6 address configured for Ethernet interface 0 (6to4 address 2002:c0a8:6301:1::/64) is used as the IPv6 address of tunnel 0:

```
Router(config)# interface tunnel 0
Router(config-if)# ipv6 unnumbered ethernet 0
Router(config-if)# tunnel source ethernet 0
Router(config-if)# tunnel mode ipv6ip 6to4
Router(config-if)# exit
Router(config)# interface ethernet 0
Router(config-if)# ipv6 address 2002:c0a8:6301:1::/64 eui-64
Router(config-if)# ipv6 address 3ffe:1234:5678::1/64
```

6RD Tunnel Example

The following sample output shows the running configuration of a 6RD tunnel:

```
Router(config)# interface Tunnel1
Router(config-if)# ipv6 address 2001:B000:100::1/32
Router(config-if)# tunnel source GigabitEthernet2/0/0
Router(config-if)# tunnel mode ipv6ip 6rd
Router(config-if)# tunnel 6rd prefix 2001:B000::/32
Router(config-if)# tunnel 6rd common prefix-len 16 suffix-len 8

Router# show tunnel 6rd tunnel
```

```
Interface Tunnel1:
  Tunnel Source: 10.1.1.1
  6RD: Operational, V6 Prefix: 2001:B000::/32
       V4 Common Prefix Length: 16, Value: 10.1.0.0
       V4 Common Suffix Length: 8, Value: 0.0.0.1
```

ISATAP Tunnel Example

The following command shows an ISATAP tunnel configured on interface Ethernet 0. Router advertisements are enabled to allow client autoconfiguration.

```
Router(config)# interface Ethernet 0
Router(config-if)# ip address 10.1.1.1 255.255.255.0
Router(config)# interface Tunnel 0
Router(config-if)# tunnel source ethernet 0
Router(config-if)# tunnel mode ipv6ip isatap
Router(config-if)# ipv6 address 2001:0DB8::/64 eiu-64
Router(config-if)# no ipv6 nd suppress-ra
```

Related Commands

Command	Description
ip address	Specifies the IP address of an IPv4 interface.
ipv6 unnumbered	Enables IPv6 processing on an interface without assigning an explicit IPv6 address to the interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.
tunnel destination	Sets the destination address for a tunnel interface.
tunnel source	Sets the source address for a tunnel interface.

tunnel source

To set the source address for a tunnel interface, use the **tunnel source** command in interface configuration mode. To remove the source address, use the **no** form of this command.

tunnel source {*ip-address* | *ipv6-address* | *interface-type interface-number*}

no tunnel source

Syntax Description

ip-address	IP address to use as the source address for packets in the tunnel. • In the case of traffic engineering (TE) tunnels it is the control packets that are affected.
ipv6-address	IPv6 address to use as the source address for packets in the tunnel.
interface-type	Interface type.
interface-number	Port, connector, or interface card number. The numbers are assigned at the factory at the time of installation or when added to a system and can be displayed with the **show interfaces** command.

Command Default

No tunnel interface source address is set.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
10.0	This command was introduced.
12.3(7)T	The address field has been updated to accept IPv6 addresses as the source address to allow an IPv6 node to be used as a tunnel source.
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.
12.2(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 Release 2.1 and implemented on Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

The source address is either an explicitly defined IP address or the IP address assigned to the specified interface.

You cannot have two tunnels using 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. This restriction is applicable only for generic routing encapsulation (GRE) tunnels. You can have more than one TE tunnel with the same source and destination address.

When using tunnels to Cayman boxes, you must set the **tunnel source** command to an explicit IP address on the same subnet as the Cayman box, not the tunnel itself.

GRE tunnel encapsulation and deencapsulation for multicast packets are handled by the hardware in PFC3 and 12.2(18)SXF and later releases. Each hardware-assisted tunnel must have a unique source. Hardware-assisted tunnels cannot share a source even if the destinations are different. You should use secondary addresses on loopback interfaces or create multiple loopback interfaces to ensure the hardware-assisted tunnels do not share a source.

Examples

Cayman Tunnel Example

The following example shows how to set a tunnel source address for Cayman tunneling:

```
Router(config)# interface tunnel0
Router(config-if)# tunnel source ethernet0
Router(config-if)# tunnel destination 172.32.164.19
Router(config-if)# tunnel mode cisco1
```

GRE Tunneling Example

The following example shows how to set a tunnel source address for GRE tunneling:

```
Router(config)# interface tunnel0
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 172.32.164.19
Router(config-if)# tunnel mode gre ip
```

MPLS TE Tunnel Example

The following example shows how to set a tunnel source for a Multiprotocol Label Switching (MPLS) TE tunnel:

```
Router> enable
Router# configure terminal
Router(config)# interface tunnel 1
Router(config-if)# ip unnumbered loopback0
Router(config-if)# tunnel source loopback1
Router(config-if)# tunnel mode mpls traffic-eng
Router(config-if)# end
```

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.

validate source-mac

To check the source media access control (MAC) address against the link-layer address, use the **validate source-mac** command in Neighbor Discovery (ND) inspection policy configuration mode.

validate source-mac

no validate source-mac

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

ND inspection policy configuration (config-nd-inspection)
RA guard policy configuration (config-ra-guard)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

When the router receives an ND message that contains a link-layer address, the source MAC address is checked against the link-layer address. Use the **validate source-mac** command to drop the packet if the link-layer address and the MAC addresses are different from each other.

Examples

The following example enables the router to drop an ND message whose link-layer address does not match the MAC address:

```
Router(config)# ipv6 nd inspection policy policy1
Router(config-nd-inspection)# validate source-mac
```

Related Commands

Command	Description
ipv6 nd inspection policy	Defines the ND inspection policy name and enters ND inspection policy configuration mode.
ipv6 nd raguard policy	Defines the RA guard policy name and enter RA guard policy configuration mode.

variance (EIGRP)

To control load balancing in an internetwork based on the Enhanced Interior Gateway Routing Protocol (EIGRP), use the **variance** command in router configuration mode or address-family topology configuration mode. To reset the variance to the default value, use the **no** form of this command.

variance *multiplier*

no variance

Syntax Description

multiplier	Metric value used for load balancing. It can be a value from 1 to 128. The default is 1, which means equal-cost load balancing.

Command Default

EIGRP uses equal-cost load balancing.

Command Modes

Router configuration (config-router)
Address-family topology configuration (config-router-af-topology)

Command History

Release	Modification
10.0	This command was introduced.
12.4(6)T	Support for IPv6 was added.
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.
15.0(1)	This command was modified. Address-family topology configuration mode was added.
12.2(33)SRE	This command was modified. Address-family topology configuration mode was added.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

Setting a variance value enables EIGRP to install multiple loop-free routes with unequal cost in a local routing table. A route learned through EIGRP must meet two criteria to be installed in the local routing table:

- The route must be loop- free. This condition is satisfied when the reported distance is less than the total distance or when the route is a feasible successor.
- The metric of the route must be lower than the metric of the best route (the successor) multiplied by the variance configured on the router.

Thus, if the variance is set to 1, only routes with the same metric as the successor are installed in the local routing table. If the variance is set to 2, any EIGRP-learned route with a metric less than 2 times the successor metric will be installed in the local routing table.

Note EIGRP does not load-share between multiple routes; it only installs the routes in the local routing table. Then, the local routing table enables switching hardware or software to load-share between the multiple paths.

Examples

The following example sets a variance value of 4:

```
Router(config)# router eigrp 109
Router(config-router)# variance 4
```

The following example sets a variance value of 4 in address-family topology configuration mode:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# network 10.0.0.0
Router(config-router-af)# topology base
Router(config-router-af-topology)# variance 4
```

virtual-profile virtual-template

To enable virtual profiles by virtual interface template, use the **virtual-profile virtual-template** command in global configuration mode. To disable this function, use the **no** form of this command.

virtual-profile virtual-template *number*

no virtual-profile virtual-template *number*

Syntax Description

number	Number of the virtual template to apply, ranging from 1 to 30.

Defaults

Disabled. No virtual template is defined, and no default virtual template number is used.

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.

Usage Guidelines

When virtual profiles are configured by virtual templates only, any interface-specific configuration information that is downloaded from the AAA server is ignored in configuring the virtual access interface for a user.

The **interface virtual-template** command defines a virtual template to be used for virtual profiles. Because several virtual templates might be defined for different purposes on the router (such as MLP, PPP over ATM, and virtual profiles), it is important to be clear about the virtual template number to use in each case.

Examples

The following example configures virtual profiles by virtual templates only. The number 2 was chosen because virtual template 1 was previously defined for use by Multilink PPP.

```
virtual-profile virtual-template 2
```

Related Commands

Command	Description
interface virtual-template	Creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces.

voice-class sip anat

To enable Alternative Network Address Types (ANAT) on a Session Initiation Protocol (SIP) trunk, use the **voice-class sip anat** command in SIP configuration or dial peer configuration mode. To disable ANAT on SIP trunks, use the **no** form of this command.

voice-class sip anat [**system**]

no voice-class sip anat [**system**]

Syntax Description

system	(Optional) Configures ANAT globally.

Command Default

ANAT is enabled on SIP trunks.

Command Modes

SIP configuration (conf-serv-sip)
Dial peer configuration (config-dial-peer)

Command History

Release	Modification
12.4(22)T	This command was introduced.

Usage Guidelines

Both the Cisco IOS SIP gateway and Cisco Unified Border Element are required to support the Session Description Protocol (SDP) ANAT semantics. The **bind** command allows the use of ANAT semantics in outbound SDP. SDP ANAT semantics are intended to address scenarios that involve different network address families (for example, different IPv4 versions). Media lines grouped using ANAT semantics provide alternative network addresses of different families for a single logical media stream. The entity creating a session description with an ANAT group must be ready to receive or send media over any of the grouped “m” lines.

By default, ANAT is enabled on SIP trunks. However, if the SIP gateway is configured in IPv4-only mode or IPv6-only mode, the gateway will not use ANAT semantics in its SDP offer.

The **system** keyword configures ANAT on all network dial peers, including the local dial peer. Using the **voice-class sip anat** command without the **system** keyword enables ANAT only for the local dial peer.

Examples

The following example globally enables ANAT on a SIP trunk:

```
Router(config-serv-sip)# voice-class sip anat system
```

The following example enables ANAT on a specified dial peer:

```
Router(config-dial-peer)# voice-class sip anat
```

Related Commands

Command	Description
bind	Binds the source address for signaling and media packets to the IPv4 or IPv6 address of a specific interface.

voice-class sip outbound-proxy

To configure an outbound proxy, use the **voice-class sip outbound-proxy** command in dial peer configuration mode. To reset the outbound proxy value to its default, use the **no** form of this command.

voice-class sip outbound-proxy {**dhcp** | **ipv4:***ipv4-address* | **ipv6:[***ipv6-address***]** | **dns:***host***:***domain*} [**:***port-number*]

no voice-class sip outbound-proxy

Syntax Description

dhcp	Specifies that the outbound-proxy IP address is retrieved from a DHCP server.
ipv4:*ipv4-address*	Configures proxy on the server, sending all initiating requests to the specified IPv4 address destination. The colon is required.
ipv6:[*ipv6-address***]**	Configures proxy on the server, sending all initiating requests to the specified IPv6 address destination. Brackets must be entered around the IPv6 address. The colon is required.
dns:*host***:***domain*	Configures proxy on the server, sending all initiating requests to the specified domain destination. The colons are required.
:*port-number*	(Optional) Port number for the Session Initiation Protocol (SIP) server. The colon is required.

Command Default

An outbound proxy is not configured.

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
12.4(15)T	This command was introduced.
12.4(22)T	This command was modified. Support for IPv6 was added.
12.4(22)YB	This command was modified. The **dhcp** keyword was added.
15.0(1)M	This command was integrated in Cisco IOS Release 15.0(1)M.

Usage Guidelines

The **voice-class sip outbound-proxy** command, in dial peer configuration mode, takes precedence over the command in SIP global configuration mode.

Brackets must be entered around the IPv6 address.

Examples

The following example shows how to configure the **voice-class sip outbound-proxy** command on a dial peer to generate an IPv4 address (10.1.1.1) as an outbound proxy:

```
Router> enable
Router# configure terminal
Router(config)# dial-peer voice 111 voip
Router(config-dial-peer)# voice-class sip outbound-proxy ipv4:10.1.1.1
```

The following example shows how to configure the **voice-class sip outbound-proxy** command on a dial peer to generate a domain (sipproxy:cisco.com) as an outbound proxy:

```
Router> enable
Router# configure terminal
Router(config)# dial-peer voice 111 voip
Router(config-dial-peer)# voice-class sip outbound-proxy dns:sipproxy:cisco.com
```

The following example shows how to configure the **voice-class sip outbound-proxy** command on a dial peer to generate an outbound proxy using DHCP:

```
Router> enable
Router# configure terminal
Router(config)# dial-peer voice 111 voip
Router(config-dial-peer)# voice-class sip outbound-proxy dhcp
```

Related Commands

Command	Description
dial-peer voice	Defines a particular dial peer, specifies the method of voice encapsulation, and enters dial peer configuration mode.
voice service	Enters voice-service configuration mode and specifies a voice encapsulation type.

voice-class source interface

To allow a loopback interface to be associated with a VoIP or VoIPv6 dial-peer profile, use the **voice-class source interface** command in dial peer configuration mode. To disable this association, use the **no** form of this command.

voice-class source interface loopback *interface-id* [*ipv4-address* | *ipv6-address*]

no voice-class source interface loopback *interface-id* [*ipv4-address* | *ipv6-address*]

Syntax Description

loopback	Specifies the loopback interface address.
interface-id	Specifies the interface on which the address is to be configured.
ipv4-address	(Optional) IPv4 address used in the loopback interface address.
ipv6-address	(Optional) IPv6 address used in the loopback interface address.

Command Default

No loopback interface is associated with a VoIPv6 dial-peer profile.

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
12.4(22)T	This command was introduced.

Usage Guidelines

When the **voice-class source interface** command is configured, the source address of Routing Table Protocol (RTP) generated by the gateway is taken from the address configured under the loopback interface. This command is used for policy-based routing (PBR) of voice packets originated by the gateway. The policy route map is configured under the loopback interface, and then the loopback interface is specified under the VoIP or VoIPv6 dial peer.

Examples

The following example associates a loopback interface with a VoIPv6 dial-peer profile:

```
Router(config)# dial-peer voice 1 voip
Router (config-dial-peer)# voice-class source interface loopback0
```

Related Commands

Command	Description
dial-peer voice	Defines a particular dial peer, specifies the method of voice encapsulation, and enters dial peer configuration mode.

voice service

To enter voice-service configuration mode and to specify a voice-encapsulation type, use the voice service command in global configuration mode..

voice service {**pots** | **voatm** | **vofr** | **voip**}

Syntax Description

pots	Telephony voice service.
voatm	Voice over ATM (VoATM) encapsulation.
vofr	Voice over Frame Relay (VoFR) encapsulation.
voip	Voice over IP (VoIP) encapsulation.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)XA	This command was introduced on the Cisco MC3810.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T for VoIP on the Cisco 2600 series and the Cisco 3600 series.
12.1(3)XI	This command was implemented on the Cisco AS5300.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.1(5)XM	This command was implemented on the Cisco AS5800.
12.1(5)XM2	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 7200 series.
12.2(11)T	This command was implemented on the Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850.

Usage Guidelines

Voice-service configuration mode is used for packet telephony service commands that affect the gateway globally.

Examples

The following example enters voice-service configuration mode for VoATM service commands:

```
voice service voatm
```

vpn

To specify that the source and destination IPv4 addresses of a given virtual private dialup network (VPDN) group belong to a specified Virtual Private Network (VPN) routing and forwarding (VRF) instance, use the **vpn** command in VPDN group or VPDN template configuration mode. To disassociate all IPv4 addresses in a VPDN group from a VRF, use the **no** form of this command.

vpn {**vrf** *vrf-name* | **id** *vpn-id*}

no vpn

Syntax Description

vrf *vrf-name*	Name of the VRF instance to be associated with the IPv4 addresses of the VPDN group.
id *vpn-id*	VPN ID of the VRF to be associated with the IPv4 addresses of the VPDN group.

Command Default

VPDN groups are not associated with a VRF.

Command Modes

VPDN group configuration
VPDN template configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.3(7)XI7	This command was integrated into Cisco IOS Release 12.3(7)XI7 and implemented on the Cisco 10000 series routers.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB for the PRE2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was implemented on the Cisco 10000 series router for the PRE3.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Use the **vpn** command to configure the Cisco IOS software to look up a VPDN source or destination IPv4 address in a specific VPN routing table instead of the global routing table.

Before you can issue the **vpn** command, a VRF instance must be created using the **ip vrf** command.

The **vpn** command can be used with both dial-in and dial-out VPDN scenarios.

Examples

The following example associates the IP addresses configured in the VPDN group named group1 with the VRF named vrf-second:

```
vpdn-group group1
```

```
 request-dialin
 protocol l2tp
!
 vpn vrf vrf-second
 source-ip 172.16.1.9
 initiate-to ip 172.16.1.1
```

The following example associates the IP addresses configured in the VPDN group named group2 with the VPN ID 11:2222:

```
vpdn-group group2
 request-dialin
 protocol l2tp
!
 vpn id 11:2222
 source-ip 172.16.1.9
 initiate-to ip 172.16.1.1
```

Related Commands

Command	Description
ip vrf	Configures a VRF routing table.
show ip route	Displays all static IP routes, or those installed using the AAA route download function.
show vpdn session	Displays session information about active Layer 2 sessions for a VPDN.
show vpdn tunnel	Displays information about active Layer 2 tunnels for a VPDN.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.
vpdn-template	Creates a VPDN template and enters VPDN template configuration mode.

vrf (DHCPv6 pool)

To associate a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) address pool with a virtual private network (VPN) routing and forwarding (VRF) instance, use the **vrf** command in DHCPv6 pool configuration mode. To remove the VRF name, use the **no** form of this command.

vrf *name*

no vrf *name*

Syntax Description

name	Name of the VRF with which the address pool is associated.

Command Default

No VRF is associated with the DHCPv6 address pool.

Command Modes

DHCPv6 pool configuration (config-dhcp)

Command History

Release	Modification
15.1(2)S	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Examples

The following example shows how to configure an IPv6 pool named pool1, and associate pool1 with a VRF instance named vrf1:

```
Router(config)# ipv6 dhcp pool pool1
# vrf vrf1
```

Related Commands

Command	Description
ipv6 dhcp pool	Configures a DHCPv6 configuration information pool and enters DHCPv6 pool configuration mode.

vrf definition

To configure a virtual routing and forwarding (VRF) routing table instance and enter VRF configuration mode, use the **vrf definition** command in global configuration mode. To remove a VRF routing table, use the **no** form of this command.

vrf definition *vrf-name*

no vrf definition *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
12.2(33)SRB	This command was introduced.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.
Cisco IOS XE Release 3.2S	This command was modified. Its use was expanded to support virtual networks.

Usage Guidelines

Use the **vrf definition** command to give a VRF a name and to enter VRF configuration mode. Once the router is in VRF configuration mode, use the **rd** command to give the VRF a route distinguisher (RD). The **rd** command creates the routing and forwarding tables and associates the RD with the VRF instance named in the *vrf-name* argument.

Users can configure shared route targets (import and export) between IPv4 and IPv6. This feature is useful in a migration scenario, where IPv4 policies already are configured and IPv6 policies should be the same as the IPv4 policies. You can configure separate route-target policies for IPv4 and IPv6 VPNs in address family configuration mode. Enter address family configuration mode from VRF configuration mode.

In VRF configuration mode, you can also associate a Simple Network Management Protocol (SNMP) context with the named VRF and configure or update a VPN ID.

The **vrf definition default** command can be used to configure a VRF name that is a NULL value until a default VRF name can be configured. This is typically before any VRF-related AAA commands are configured.

Virtual Network Use of vrf definition Command

Use the **vrf definition** command to give a VRF a name and to enter VRF configuration mode. By default, each virtual network trunk interface on the router is able to carry traffic for every VRF defined by the **vrf definition** command. If you want to enable only a subset of VRFs on a trunk interface, use the **vrf list** command.

Note We recommend you do not define a virtual network with the name "global," because the system predefines **vnet globa**l and it is best to avoid conflict with the predefined version.

Examples

The following example assigns the name vrf1 to a VRF, enters VRF configuration mode, and configures a route distinguisher, 100:20:

```
Router(config)# vrf definition vrf1
Router(config-vrf)# rd 100:20
```

The following virtual network example defines VRF red, enters VRF configuration mode, and assigns virtual network tag 100 to VRF red:

```
Router(config)# vrf definition red
Router(config-vrf)# vnet tag 100
```

Related Commands

Command	Description
address-family (VRF)	Enters VRF address family configuration mode to select an address family type for a VRF table.
context	Associates an SNMP context with a particular VRF.
rd	Specifies a route distinguisher.
route-target	Creates a route-target extended community for a VPN VRF.
vnet	Configures overrides of an interface's attributes on a per-VRF basis
vnet tag	Assigns a tag to a virtual network.
vpn id	Sets or updates a VPN ID on a VRF.
vrf forwarding	Associates a VRF instance with an interface or subinterface.
vrf list	Defines a list of VRFs.

vrf forwarding

To associate a Virtual Routing and Forwarding (VRF) instance or a virtual network with an interface or subinterface, use the **vrf forwarding** command in interface configuration mode. To disassociate a VRF or virtual network from an interface, use the **no** form of this command.

vrf forwarding *vrf-name* [**downstream** *vrf-name2*]

no vrf forwarding

Syntax Description

vrf-name	The interface name to be associated with the specified VRF.
downstream	(Optional) Enables half-duplex VRF (HDVRF) functionality on the interface and associates the interface with the downstream VRF.
vrf-name2	(Optional) The interface name to be associated with the specified downstream VRF.

Command Default

The default for an interface is the global routing table.

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.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB. The **downstream** *vrf-name2* keyword and argument were added to support Multiprotocol Label Switching VPN half-duplex VRFs.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.
Cisco IOS XE Release 3.2S	This command was modified. Its use was expanded to support virtual networks.

Usage Guidelines

Use the **vrf forwarding** command to associate an interface with a VRF. When the interface is bound to a VRF, previously configured IPv4 and IPv6 addresses are removed, and they must be reconfigured.

The **downstream** keyword associates the interfaces with a downstream VRF, which enables half-duplex VRF functionality on the interface. Some functions operate in the upstream VRFs, and others operate in the downstream VRFs. The following functions operate in the downstream VRFs:

- PPP peer routes are installed in the downstream VRFs.
- Authentication, authorization, and accounting (AAA) per-user routes are installed in the downstream VRFs.

- A Reverse Path Forwarding (RPF) check is performed in the downstream VRFs.

In the virtual network environment, the **vrf forwarding** command is supported on an edge interface; it is not supported on a trunk interface.

A VRF and a virtual network are mutually exclusive on an interface. In other words, an interface can be a VRF interface or a virtual network edge interface, but not both.

Examples

The following example shows how to associate a VRF named site1 to serial interface 0/0 and configure an IPv6 and an IPv4 address:

```
interface Serial0/0
 vrf forwarding site1
 ipv6 address 2001:100:1:1000::72b/64
 ip address 10.11.11.1 255.255.255.0
```

The following example associates the VRF named U with the virtual-template 1 interface and specifies the downstream VRF named D:

```
Router(config)# interface virtual-template 1
Router(config-if)# vrf forwarding U downstream D
Router(config-if)# ip unnumbered Loopback1
```

The following example shows how to configure an edge interface:

```
interface gigabitethernet 0/0/0
 vrf forwarding red
 ip address 10.12.12.1 255.255.255.0
```

Related Commands

Command	Description
vnet	Enters virtual network interface mode.
vrf definition	Configures a VRF routing table instance and enters VRF configuration mode.

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.
15.1(2)T	Support for IPv6 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.

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)

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.
15.1(2)T	Support for IPv6 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.