



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 <i>level</i>	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.
<i>list-name</i>	Character string used to name the list of at least one of the following accounting methods: <ul style="list-style-type: none"> 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 <i>group-name</i>—Uses a subset of RADIUS or TACACS+ servers for accounting as defined by the server group <i>group-name</i> argument.
guarantee-first	Guarantees system accounting as the first record.
vrf <i>vrf-name</i>	(Optional) Specifies a virtual routing and forwarding (VRF) configuration. VRF is used <i>only</i> 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 <i>group-name</i>	Specifies the accounting method list. Enter at least one of the following keywords: <ul style="list-style-type: none"> • 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 <i>vrf-name</i> 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 <i>vrf-name</i> 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 <i>group-name</i>	Uses a subset of RADIUS or TACACS+ servers for accounting as defined by the server group <i>group-name</i> 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.	
<i>method1, method2, method3, method4</i>	(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.
<i>list-name</i>	Character string used to name the list of authentication methods tried when a user logs in.
<i>method1 [method2...]</i>	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.
12.2(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 <i>group-name</i>	Uses a cache server group for authentication.
group <i>group-name</i>	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.
<i>level</i>	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.
<i>list-name</i>	Character string used to name the list of authorization methods.
<i>method1</i> [<i>method2</i> ...]	(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 <i>group-name</i>	Uses a cache server group for authorization.
group <i>group-name</i>	Uses a subset of RADIUS or TACACS+ servers for accounting as defined by the server group <i>group-name</i> 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 <i>group-name</i>	Uses a subset of RADIUS servers for accounting as defined by the server group <i>group-name</i> 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

<i>group-name</i>	Character string used to name the group of servers. See Table 5 for a list of words that cannot be used as the <i>group-name</i> 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

<i>group-name</i>	Character string used to name the group of servers. See Table 5 for a list of words that cannot be used as the <i>group-name</i> 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

<i>start-time</i>	Beginning time that the key specified by the key command is valid to be received. The syntax can be either of the following: <i>hh:mm:ss Month date year</i> <i>hh:mm:ss date Month year</i> <ul style="list-style-type: none"> • <i>hh</i>—hours • <i>mm</i>—minutes • <i>ss</i>—seconds • <i>Month</i>—first three letters of the month • <i>date</i>—date (1–31) • <i>year</i>—year (four digits) <p>The default start time and the earliest acceptable date is January 1, 1993.</p>
infinite	Key is valid to be received from the <i>start-time</i> value on.
<i>end-time</i>	Key is valid to be received from the <i>start-time</i> value until the <i>end-time</i> value. The syntax is the same as that for the <i>start-time</i> value. The <i>end-time</i> value must be after the <i>start-time</i> value. The default end time is an infinite time period.
duration <i>seconds</i>	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)SX14	Support for IPv6 was added. The prefer vlan keyword combination is not supported in 12.2(33)SX14.
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)SX14, 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

<i>ipv4-address</i>	IPv4 address of the remote peer.
<i>mask</i>	(Optional) Subnet mask.
<i>ipv6-address</i>	IPv6 address of the remote peer.
<i>prefix</i>	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

<i>ipv6-address</i>	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	<i>ipv6-address</i>	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 <i>autonomous-system-number</i>	(Optional) Specifies the autonomous system number. This keyword/argument pair is required for EIGRP named configurations.
vrf <i>vrf-name</i>	(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 <i>vrf-name</i>	(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 **address-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, igmp, 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** | **vpn6**]

no address-family ipv6 [*vrf vrf-name*] [**unicast** | **multicast** | **vpn6**]

Syntax Description

vrf	(Optional) Specifies all Virtual Private Network (VPN) routing and forwarding (VRF) instance tables or a specific VRF table for IPv6 address.
<i>vrf-name</i>	(Optional) Names a specific VRF table for an IPv6 address.
unicast	(Optional) Specifies IPv6 unicast address prefixes.
multicast	(Optional) Specifies IPv6 multicast address prefixes.
vpn6	(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 <i>vrf-name</i> 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 vpn6 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 was integrated 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		
	<i>ipv6-prefix</i>	IPv6 address prefix.
	lifetime { <i>valid-lifetime preferred-lifetime</i> 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

<i>address</i>	Aggregate address.
<i>mask</i>	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 <i>map-name</i>	(Optional) Specifies the name of the route map used to select the routes to be suppressed.
advertise-map <i>map-name</i>	(Optional) Specifies the name of the route map used to select the routes to create AS_SET origin communities.
attribute-map <i>map-name</i>	(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		
<i>from-type</i>	Originating endpoint type. The following choices are valid:	<ul style="list-style-type: none"> h323—H.323. sip—Session Interface Protocol (SIP).
to	Indicates that the argument that follows is the connection target.	
<i>to-type</i>	Terminating endpoint type. The following choices are valid:	<ul style="list-style-type: none"> 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		
<i>area-ID</i>		Area ID associated with the OSPFv3 interface.
range		Summarizes routes that match the address or address mask on border routers only.
<i>ipv6-prefix/</i> <i>prefix-length</i>		An IPv6 prefix (address) and prefix length.
virtual-link		Defines a virtual link and its parameters. <ul style="list-style-type: none"> This keyword can be used with the IPv6 address family only.
<i>router-id</i>		Router ID associated with the virtual-link neighbor. <ul style="list-style-type: none"> 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

<i>area-id</i>	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 <i>spi</i>	Security policy index (SPI) value. The <i>spi</i> 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 <i>area-id</i> argument.
sha1	Enables Secure Hash Algorithm 1 (SHA-1) authentication on the area specified by the <i>area-id</i> argument.
<i>key-encryption-type</i>	(Optional) Identifier of values that can be entered: <ul style="list-style-type: none"> 0—The key is not encrypted. 7—The key is encrypted.
<i>key</i>	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
<i>area-id</i>	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 <i>spi</i>	Security policy index (SPI) value. The <i>spi</i> value must be a number from 256 to 4294967295.
esp	Encapsulating security payload (ESP).
<i>encryption-algorithm</i>	Encryption algorithm to be used with ESP. The values can be any of the following: <ul style="list-style-type: none"> aes-cdc—Enables AES-CDC encryption 3des—Enables 3DES encryption des—Enables DES encryption null—ESP with no encryption.
<i>key-encryption-type</i>	(Optional) Identifier of values that can be entered: <ul style="list-style-type: none"> 0—The key is not encrypted. 7—The key is encrypted.
<i>key</i>	(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.
<i>authentication-algorithm</i>	Encryption authentication algorithm to be used. The values can be one of the following: <ul style="list-style-type: none"> 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 lprefix-length [advertise | not-advertise] [cost cost]
```

```
no area area-id range ipv6-prefix lprefix-length [advertise | not-advertise] [cost cost]
```

Syntax Description		
<i>area-id</i>	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.	
<i>ipv6-prefix</i>	IPv6 prefix.	
<i>lprefix-length</i>	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 <i>cost</i>	(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 <i>cost</i> argument were added.
	12.2(15)T	Support for IPv6 was added. The cost keyword and <i>cost</i> 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

<i>area-id</i>	Identifier of the area for which routes are to be summarized. It can be specified as either a decimal value or an IPv6 prefix.
<i>ip-address</i>	IP address.
<i>ip-address-mask</i>	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 <i>cost</i>	(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 <i>cost</i> argument were added.
12.2(15)T	The cost keyword and <i>cost</i> 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	
<i>area-id</i>	Area ID assigned to the virtual link. This can be either a decimal value or a valid IPv6 prefix. There is no default.
<i>router-id</i>	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 <i>seconds</i>	(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 <i>seconds</i>	(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 <i>seconds</i>	(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 <i>seconds</i>	(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 <i>hop-count</i>	(Optional) Configures Time-to-Live (TTL) security on a virtual link. The <i>hop-count</i> 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 <i>hop-count</i> 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	
<i>area-id</i>	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.
<i>router-id</i>	Router ID associated with the virtual link neighbor. The router ID appears in the show ipv6 ospf display. There is no default.
hello-interval <i>seconds</i>	(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 <i>seconds</i>	(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 <i>seconds</i>	(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 <i>seconds</i>	(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 <i>spi</i>	Security policy index (SPI) value. The <i>spi</i> value must be a number from 256 to 4294967295.
<i>authentication-algorithm</i>	Encryption authentication algorithm to be used. The values can be one of the following: <ul style="list-style-type: none"> md5—Enables Message Digest 5 (MD5). sha-1—Enables SHA-1.

<i>key-encryption-type</i>	(Optional) Identifier of values that can be entered: <ul style="list-style-type: none"> • 0—The key is not encrypted. • 7—The key is encrypted.
<i>key</i>	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	
<i>area-id</i>	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.
<i>router-id</i>	Router ID associated with the virtual link neighbor. There is no default.
hello-interval <i>seconds</i>	(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 <i>seconds</i>	(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 <i>seconds</i>	(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 <i>seconds</i>	(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 <i>spi</i>	Security policy index (SPI) value. The <i>spi</i> value must be a number from 256 to 4294967295.
esp	Encapsulating security payload (ESP).
<i>encryption-algorithm</i>	Encryption algorithm to be used with ESP. The values can be any of the following: <ul style="list-style-type: none"> aes-cdc—Enables AES-CDC encryption. 3des—Enables 3DES encryption. des—Enables DES encryption. null—ESP with no encryption.

<i>key-encryption-type</i>	(Optional) Identifier of values that can be entered: <ul style="list-style-type: none"> • 0—The key is not encrypted. • 7—The key is encrypted.
<i>key</i>	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.
<i>authentication-algorithm</i>	Encryption authentication algorithm to be used. The values can be one of the following: <ul style="list-style-type: none"> • 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	Command	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:

■ arp (interface)

```
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.
<i>profile-description-text</i>	(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 <i>profile-description-text</i> 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

<i>profile-identifier</i>	Number that identifies the DSP farm profile. Range is 1 to 65535. There is no default value.
register <i>device-name</i>	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 **atm 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	<i>protocol</i>	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:FDFE: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.
<i>hex-in</i>	Index for inbound registration packets. The range is from 100 to ffffffff.
decimal <i>decimal-in</i>	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.
<i>hex-out</i>	Index for outbound registration packets. The range is from 100 to ffffffff.
decimal <i>decimal-out</i>	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.
<i>hex-value</i>	SPI expressed as a hexadecimal number. The range is from 100 to ffffffff.
decimal <i>decimal-value</i>	SPI expressed as a decimal number. The range is from 256 to 4294967295.
key	Security key.
ascii <i>string</i>	Security key expressed as an ASCII string. A maximum of 32 characters is allowed. No spaces are allowed.
hex <i>string</i>	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.
<i>algorithm-type</i>	(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.
<i>seconds</i>	(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 10⁸ 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

<i>percent</i>	(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 <i>percent</i> 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

<i>kbps</i>	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 [<i>kbps</i>]) 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
```

■ bandwidth (interface)

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 <i>milliseconds</i>	Specifies the rate at which BFD control packets will be sent to BFD peers. The configurable time period for the <i>milliseconds</i> argument is from 50 to 999 milliseconds (ms).
min_rx <i>milliseconds</i>	Specifies the rate at which BFD control packets will be expected to be received from BFD peers. The configurable time period for the <i>milliseconds</i> argument is from 50 to 999 ms.
multiplier <i>multiplier-value</i>	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 <i>multiplier-value</i> 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 <i>seconds</i>	(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 <i>seconds</i>	(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: <ul style="list-style-type: none"> 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 <i>internal</i> if the path is learned via iBGP. The field is <i>external</i> 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

<i>ip-address</i>	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 <i>interface-id</i>	Specifies an interface as the source address of SIP packets. Specifies one of the following interfaces: <ul style="list-style-type: none"> • 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 <i>ipv4-address</i>	(Optional) Configures the IPv4 address. Several IPv4 addresses can be configured under one interface.
ipv6-address <i>ipv6-address</i>	(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.
<i>access-list-name</i>	(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.
<i>auth-option</i>	(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.
<i>seconds</i>	(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.
<i>maximum</i>	(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.
<i>refresh</i>	(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 <i>auth-option</i> 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 be 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	<i>bridge-group</i>	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 <i>number</i>	(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 <i>minutes</i>	(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 <i>seconds</i>	(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	Parameter	Description
	ra-count	Routing advertisement (RA) count determines how many RAs to send to the MN.
	<i>ra-value</i>	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.
	<i>seconds</i>	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 <i>x</i> 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 <i>x</i> 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 <i>count-number</i>	(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 <i>seconds</i>	(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 <i>seconds</i>	(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 <i>seconds</i>	(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.

<i>class-map-name</i>	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.
<i>protocol-name</i>	Layer 7 application-specific class map. The supported protocols are as follows: <ul style="list-style-type: none"> • 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		
<i>class-map-name</i>	Name of the class on which an action is to be performed.	
	The <i>class-map-name</i> must match the appropriate class name specified via the class-map type inspect command.	
<i>protocol-name</i>	Layer 7 application-specific traffic class. The supported protocols are as follows:	
	<ul style="list-style-type: none"> • 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 or a 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		
	<i>access-list-number</i>	Access list number of the access list for which to clear the counters.
	<i>access-list-name</i>	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.
	<i>autonomous-system-number</i>	Resets BGP sessions for BGP neighbors within the specified autonomous system.
	<i>ip-address</i>	Resets the TCP connection to the specified IPv4 BGP neighbor and removes all routes learned from the connection from the BGP table.
	<i>ipv6-address</i>	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.
	<i>peer-group-name</i>	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.
<i>ipv6-prefix</i>	(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.
<i>/prefix-length</i>	(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.
<i>ipv6-prefix</i>	(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.
<i>lprefix-length</i>	(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 <i>regexp</i>	(Optional) Clears flap statistics for all the paths that match the regular expression.
filter-list <i>list</i>	(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.
<i>name</i>	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.
<i>vrf-name</i>	(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, its 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}
| fvr vrf-name | psh number]
```

Syntax Description

local { <i>ipv4-address</i> <i>ipv6-address</i> }	(Optional) Clears the IKEv2 security associations matching the local address.
remote { <i>ipv4-address</i> <i>ipv6-address</i> }	(Optional) Clears the IKEv2 security associations matching the remote address.
fvr <i>vrf-name</i>	(Optional) Clears the IKEv2 security associations matching the specified front door virtual routing and forwarding (FVR) instance.
psh <i>number</i>	(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 <i>number</i>	(Optional) Specifies the tunnel address for the DMVPN peer. The range is from 0 to 2147483647.
peer	(Optional) Specifies a DMVPN peer.
<i>ipv4-address</i>	(Optional) The IPv4 address for the DMVPN peer.
<i>FQDN-string</i>	(Optional) Next hop server (NHS) fully qualified domain name (FQDN) string.
vrf <i>vrf-name</i>	(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. <ul style="list-style-type: none"> You must use the static keyword for all NHS FQDN configurations. <p>Note If the static keyword is not specified, only dynamic NHRP entries are cleared.</p>

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 <i>ipv6-address</i> 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 <i>FQDN-string</i> 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
```

clear dmvpn session**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.
<i>autonomous-system-number</i>	(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.
<i>vrf-name</i>	(Optional) Name of the VRF address-family to which the command is applied.
<i>ip-address</i>	(Optional) IPv4 or IPv6 address of the neighbor. Specifying an address removes all entries with this address from the neighbor table.
<i>interface-type</i>	(Optional) Interface type. Specifying this argument removes the specified interface type that all entries learned via this interface from the neighbor table.
<i>interface-number</i>	(Optional) Interface number. Specifying this arguments removes the specified interface number that all entries learned via this interface from the neighbor table.
<i>soft</i>	(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	<i>access-list-number</i> <i>access-list-name</i>	(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	<i>access-list-name</i>	(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.

clear ipv6 access-list

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	
<i>ipv6-address</i>	(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 <i>vrf-name</i>	(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 <i>vrf-name</i> keyword and argument were added.
	Cisco IOS XE Release 3.3S	This command was modified. The vrf <i>vrf-name</i> 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	<i>interface-type</i>	Interface type and number. For more information, use the question mark (?) online help function.
	<i>interface-number</i>	

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: <pre>Router# clear ipv6 dhcp client Ethernet 1/0</pre>
-----------------	---

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.
<i>ipv6-address</i>	Clears the host IPv6 address that contains the conflicting address.
vrf <i>vrf-name</i>	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 <i>vrf-name</i> keyword and argument were added.
Cisco IOS XE Release 3.3S	This command was modified. The vrf <i>vrf-name</i> 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		
<i>ipv6-address</i>	(Optional)	The address of a DHCP for IPv6 relay client.
vrf <i>vrf-name</i>	(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 <i>vrf-name</i> keyword and argument were added.
	Cisco IOS XE Release 3.3S	This command was modified. The vrf <i>vrf-name</i> 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		
<i>as-number</i>	(Optional)	Autonomous system number.
neighbor	(Optional)	Deletes neighbor router entries.
<i>ipv6-address</i>	(Optional)	IPv6 address of a neighboring router.
<i>interface-type</i>	(Optional)	The interface type of the neighbor router.
<i>interface-number</i>	(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 <i>session-number</i>	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 <i>vrf-name</i>	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
<i>group-name</i> <i>group-address</i>	(Optional) IPv6 address or name of the multicast group.
<i>source-address</i> <i>source-name</i>	(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 <i>vrf-name</i> 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 <i>vrf-name</i>	(Optional)	Specifies a virtual routing and forwarding (VRF) configuration.
<i>interface-type</i>	(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 <i>vrf-name</i> 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.
<i>prefix</i>	(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.
<i>interface-type</i> <i>interface-number</i>	(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
```

clear ipv6 mobile binding

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

<i>interface-type</i>	(Optional) Interface type and number.
<i>interface-number</i>	

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.