mpls traffic-eng auto-bw timers

To enable automatic bandwidth adjustment for a platform and to start output rate sampling for tunnels configured for automatic bandwidth adjustment, use the **mpls traffic-eng auto-bw timers** command in global configuration mode. To disable automatic bandwidth adjustment for the platform, use the **no** form of this command.

mpls traffic-eng auto-bw timers [**frequency** *seconds*]

no mpls traffic-eng auto-bw timers

Syntax Description

frequency *seconds*	(Optional) Interval, in seconds, for sampling the output rate of each tunnel configured for automatic bandwidth. The value must be from 1 through 604800. The recommended value is 300.

Command Default

When the optional **frequency** keyword is not specified, the sampling interval is 300 seconds (5 minutes).

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(11)S	This command was integrated into Cisco IOS Release 12.2(11)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

The **mpls traffic-eng auto-bw timers** command enables automatic bandwidth adjustment on a platform by causing traffic engineering to periodically sample the output rate for each tunnel configured for bandwidth adjustment.

The **no mpls traffic-eng auto-bw timers** command disables automatic bandwidth adjustment for a platform by terminating the output rate sampling and bandwidth adjustment for tunnels configured for adjustment. In addition, the **no** form of the command restores the configured bandwidth for each tunnel where "configured bandwidth" is determined as follows:

- If the tunnel bandwidth was explicitly configured via the **tunnel mpls traffic-eng bandwidth** command after the running configuration was written (if at all) to the startup configuration, the "configured bandwidth" is the bandwidth specified by that command.
- Otherwise, the "configured bandwidth" is the bandwidth specified for the tunnel in the startup configuration.

Examples

The following example shows how to designate that for each Multiprotocol Label Switching (MPLS) traffic engineering tunnel, the output rate is sampled once every 10 minutes (every 600 seconds):

```
Router(config)# mpls traffic-eng auto-bw timers frequency 600
```

Related Commands

Command	Description
tunnel mpls traffic-eng auto-bw	Enables automatic bandwidth adjustment for a tunnel, specifies the frequency with which tunnel bandwidth can be automatically adjusted, and designates the allowable range of bandwidth adjustments.
tunnel mpls traffic-eng bandwidth	Configures bandwidth required for an MPLS traffic engineering tunnel.

multi-topology

To enable multitopology Intermediate System-to-Intermediate System (IS-IS) for IPv6, use the **multi-topology** command in address family configuration mode. To disable multitopology IS-IS for IPv6, use the **no** form of this command.

multi-topology [**transition**]

no multi-topology

Syntax Description

transition	(Optional) Allows an IS-IS IPv6 user to continue to use single shortest path first (SPF) mode while upgrading to multitopology IS-IS for IPv6.

Command Default

Multitopology IS-IS is disabled by default.

Command Modes

Address family configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.6	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

By default, the router runs IS-IS IPv6 in single SPF mode. The **multi-topology** command enables multitopology IS-IS for IPv6.

The optional **transition** keyword can be used to migrate from IS-IS IPv6 single SPF mode to multitopology IS-IS IPv6. When transition mode is enabled, the router advertises both multitopology type, length, and value (TLV) objects and single-SPF-mode IS-IS IPv6 TLVs, but the SPF is computed using the single-SPF-mode IS-IS IPv6 TLV. This action has the side effect of increasing the link-state packet (LSP) size.

Examples

The following example enables multitopology IS-IS for IPv6:

```
Router(config)# router isis
Router(config-router)# address-family ipv6
Router(config-router-af)# multi-topology
```

nai

To specify the network address identifier (NAI) for the IPv6 mobile node, use the **nai** command in home agent configuration mode or IPv6 mobile router host configuration mode. To remove a host configuration, use the **no** form of this command.

nai [**realm** | **user** | **macaddress**] {*user@realm* | *@realm*}

no nai

Syntax Description

realm	(Optional) A realm is to be used as the NAI.
user	(Optional) A user address is to be used as the NAI.
macaddress	(Optional) A MAC address is to be used as the NAI.
user@realm	Fully qualified specific user address and realm.
@realm	Any user address at a specific realm.

Command Default

No NAI is specified.

Command Modes

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

Command History

Release	Modification
12.4(11)T	This command was introduced.
12.2(33)SRB	Support for IPv6 was added.
12.4(20)T	IPv6 network mobility (NEMO) functionality was added.

Usage Guidelines

The **nai** command can be used to configure a specific user NAI or a generic realm for defining a group.

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

```
host group group1
  nai  @cisco.com
  address baba::1
```

Two different profiles cannot be configured with the **nai** command configured with the same *@realm* value. For example, the following two profiles are configured with the same NAI realm of @cisco.com, which is not valid:

```
host group group1
  nai  @cisco.com

host group group2
  nai  @cisco.com
```

However, if the one of the profiles uses a fully qualified NAI, which is configured using the **nai** command with the *user@realm* argument, its properties take precedence over the group profile for that user, and the second group's configuration using the **nai** command with the *@realm* argument is valid.

```
host group group1
  nai example@cisco.com
host group group2
  nai  @cisco.com
```

Examples

In the following example, the host group named group1 is configured using the NAI fully qualified realm of example@cisco.com:

```
host group group1
  nai example@cisco.com
```

Related Commands

Command	Description
host group	Creates a host configuration in IPv6 Mobile.
ipv6 mobile home-agent (global configuration)	Enters home agent configuration mode.

neighbor (EIGRP)

To define a neighboring router with which to exchange routing information on a router that is running Enhanced Interior Gateway Routing Protocol (EIGRP), use the **neighbor** command in router configuration mode or address-family configuration mode. To remove an entry, use the **no** form of this command.

neighbor {*ip-address* | *ipv6-address*} *interface-type interface-number* [**remote** *maximum-hops*]

no neighbor {*ip-address* | *ipv6-address*} *interface-type interface-number*

Syntax Description

ip-address	IP address of a peer router with which routing information will be exchanged.
ipv6-address	IPv6 address of a peer router with which routing information will be exchanged.
interface-type	Interface through which peering is established.
interface-number	Number of the interface or subinterface.
remote	(Optional) Specifies that the neighbor is remote. This keyword is available only for loopback interfaces.
maximum-hops	(Optional) Maximum hop count. Valid range is 3 to 100. This argument is available only when the **remote** keyword is configured.

Command Default

No neighboring routers are defined.

Command Modes

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

Command History

Release	Modification
10.0	This command was introduced.
12.4(6)T	The *ipv6-address* argument was added.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	This command was modified. Address-family configuration mode was added.
12.2(33)SRE	This command was modified. Address-family configuration mode was added.
Cisco IOS XE Release 2.5.	This command was modified. Address-family configuration mode was added.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

Multiple neighbor statements can be used to establish peering sessions with specific EIGRP neighbors. The interface through which EIGRP will exchange routing updates must be specified in the neighbor statement. The interfaces through which two EIGRP neighbors exchange routing updates must be configured with IP addresses from the same network.

Note Configuring the **passive-interface** command suppresses all incoming and outgoing routing updates and hello messages. EIGRP neighbor adjacencies cannot be established or maintained over an interface that is configured as passive.

Examples

The following example configures EIGRP peering sessions with the 192.168.1.1 and 192.168.2.2 neighbors:

```
Router(config)# router eigrp 1
Router(config-router)# network 192.168.0.0
Router(config-router)# neighbor 192.168.1.1 Ethernet 0/0
Router(config-router)# neighbor 192.168.2.2 Ethernet 1/1
```

The following named configuration example configures EIGRP to send address-family updates to specific neighbors:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# neighbor 192.168.1.1 ethernet0/0
Router(config-router-af)# neighbor 10.1.1.2 loopback0 remote 10
```

Related Commands

Command	Description
address-family (EIGRP)	Enters address-family configuration mode to configure an EIGRP routing instance.
ipv6 router eigrp	Configures the EIGRP for IPv6 routing process.
passive-interface	Disables sending EIGRP hello packets and disables routing updates on an interface.
router eigrp	Configures the EIGRP address-family process.

neighbor activate

To enable the exchange of information with a Border Gateway Protocol (BGP) neighbor, use the **neighbor activate** command in address family configuration mode or router configuration mode. To disable the exchange of an address with a BGP neighbor, use the **no** form of this command.

neighbor {*ip-address* | *peer-group-name* | *ipv6-address***%**} **activate**

no neighbor {*ip-address* | *peer-group-name* | *ipv6-address***%**} **activate**

Syntax Description

ip-address	IP address of the neighboring router.
peer-group-name	Name of the BGP peer group.
ipv6-address	IPv6 address of the BGP neighbor.
%	(Optional) IPv6 link-local address identifier. This keyword needs to be added whenever a link-local IPv6 address is used outside the context of its interface.

Command Default

The exchange of addresses with BGP neighbors is enabled for the IPv4 address family. Enabling address exchange for all other address families is disabled.

Note Address exchange for address family IPv4 is enabled by default for each BGP routing session configured with the **neighbor remote-as** command unless you configure the **no bgp default ipv4-activate** command before configuring the **neighbor remote-as** command, or you disable address exchange for address family IPv4 with a specific neighbor by using the **no** form of the **neighbor activate** command.

Command Modes

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

Command History

Release	Modification
11.0	This command was introduced.
12.0(5)T	Support for address family configuration mode and the IPv4 address family was added.
12.2(2)T	The *ipv6-address* argument and support for the IPv6 address family were added.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	The **%** keyword was added

Release	Modification
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

Use this command to advertise address information in the form of an IP or IPv6 prefix. The address prefix information is known as Network Layer Reachability Information (NLRI) in BGP.

The **%** keyword is used whenever link-local IPv6 addresses are used outside the context of their interfaces. This keyword does not need to be used for non-link-local IPv6 addresses.

Examples

Address Exchange Example for Address Family vpn4

The following example shows how to enable address exchange for address family vpnv4 for all neighbors in the BGP peer group named PEPEER and for the neighbor 10.0.0.44:

```
Router(config)# address-family vpnv4
Router(config-router-af)# neighbor PEPEER activate
Router(config-router-af)# neighbor 10.0.0.44 activate
Router(config-router-af)# exit-address-family
```

Address Exchange Example for Address Family IPv4 Unicast

The following example shows how to enable address exchange for address family IPv4 unicast for all neighbors in the BGP peer group named group1 and for the BGP neighbor 172.16.1.1:

```
Router(config)# address-family ipv4 unicast
Router(config-router-af)# neighbor group1 activate
Router(config-router-af)# neighbor 172.16.1.1 activate
```

Address Exchange Example for Address Family IPv6

The following example shows how to enable address exchange for address family IPv6 for all neighbors in the BGP peer group named group2 and for the BGP neighbor 7000::2:

```
Router(config)# address-family ipv6
Router(config-router-af)# neighbor group2 activate
Router(config-router-af)# neighbor 7000::2 activate
```

Related Commands

Command	Description
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard IPv4 address prefixes.
address-family ipv6	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard IPv6 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard VPNv4 address prefixes.
address-family vpnv6	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard VPNv6 address prefixes.

exit-address-family	Exits from the address family submode.
neighbor remote-as	Adds an entry to the BGP or multiprotocol BGP neighbor table.

neighbor ebgp-multihop

To accept and attempt BGP connections to external peers residing on networks that are not directly connected, use the **neighbor ebgp-multihop** command in router configuration mode. To return to the default, use the **no** form of this command.

neighbor {*ip-address* | *ipv6-address* | *peer-group-name*} **ebgp-multihop** [*ttl*]

no neighbor {*ip-address* | *ipv6-address* | *peer-group-name*} **ebgp-multihop**

Syntax Description

ip-address	IP address of the BGP-speaking neighbor.
ipv6-address	IPv6 address of the BGP-speaking neighbor.
peer-group-name	Name of a BGP peer group.
ttl	(Optional) Time-to-live in the range from 1 to 255 hops.

Command Default

Only directly connected neighbors are allowed.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
10.0	This command was introduced.
11.0	The *peer-group-name* argument was added.
12.2(33)SRA	The *ipv6-address* argument and support for the IPv6 address family were added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

This feature should be used only under the guidance of Cisco technical support staff.

If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command.

To prevent the creation of loops through oscillating routes, the multihop will not be established if the only route to the multihop peer is the default route (0.0.0.0).

Examples

The following example allows connections to or from neighbor 10.108.1.1, which resides on a network that is not directly connected:

```
router bgp 109
 neighbor 10.108.1.1 ebgp-multihop
```

Related Commands

Command	Description
neighbor advertise-map non-exist-map	Allows a BGP speaker (the local router) to send the default route 0.0.0.0 to a neighbor for use as a default route.
neighbor peer-group (creating)	Creates a BGP peer group.
network (BGP and multiprotocol BGP)	Specifies the list of networks for the BGP routing process.

neighbor next-hop-unchanged

To enable an external BGP (eBGP) peer that is configured as multihop to propagate the next hop unchanged, use the **neighbor next-hop-unchanged** command in address family or router configuration mode. To disable that propagation of the next hop being unchanged, use the **no** form of this command.

neighbor {*ip-address* | *ipv6-address* | *peer-group-name*} **next-hop-unchanged** [**allpaths**]

no neighbor {*ip-address* | *ipv6-address* | *peer-group-name*} **next-hop-unchanged** [**allpaths**]

Syntax Description

ip-address	Propagate the iBGP path's next hop unchanged for this IPv4 neighbor.
ipv6-address	Propagate the iBGP path's next hop unchanged for this IPv6 neighbor.
peer-group-name	Propagate the iBGP path's next hop unchanged for this BGP peer group.
allpaths	(Optional) Propagate the next hop unchanged, for all paths (iBGP and eBGP) to this neighbor.

Command Default

This command is disabled by default.

Command Modes

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

Command History

Release	Modification
12.0(16)ST	This command was introduced.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was modified. The **allpaths** keyword was added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

By default, for eBGP, the next hop to reach a connected network is the IP address of the neighbor that sent the update. Therefore, as an update goes from router to router, the next hop typically changes to be the address of the neighbor that sent the update (the router's own address).

However, there might be a scenario where you want the next hop to remain unchanged. The **neighbor next-hop-unchanged** command is used to propagate the next hop unchanged for multihop eBGP peering sessions. This command is configured on an eBGP neighbor, but the neighbor propagates routes learned from iBGP; that is, the neighbor propagates the next hop of iBGP routes toward eBGP.

Caution Using the **neighbor next-hop-unchanged** command or incorrectly altering the BGP next hop can cause inconsistent routing, routing loops, or a loss of connectivity. It should only be attempted by someone who has a good understanding of the design implications.

This command can be used to configure MPLS VPNs between service providers by not modifying the next hop attribute when advertising routes to an eBGP peer.

Examples

The following example configures a multihop eBGP peer at 10.0.0.100 in a remote autonomous system (AS). When the local router sends updates to that peer, it will send them without modifying the next hop attribute.

```
router bgp 65535
 address-family ipv4
 neighbor 10.0.0.100 remote-as 65600
 neighbor 10.0.0.100 activate
 neighbor 10.0.0.100 ebgp-multihop 255
 neighbor 10.0.0.100 next-hop-unchanged
 end
```

Related Commands

Command	Description
address-family ipv4	Enters address family configuration mode for configuring routing sessions, such as BGP, RIP, or static routing sessions, that use standard IPv4 address prefixes.
address-family vpnv4	Enters address family configuration mode for configuring routing sessions, such as BGP, RIP, or static routing sessions, that use standard VPNv4 address prefixes.
neighbor ebgp-multihop	Accepts and attempts BGP connections to external peers residing on networks that are not directly connected.
neighbor next-hop-self	Configures the router as the next hop for a BGP-speaking neighbor or peer group.

neighbor override-capability-neg

To enable the IPv6 address family for a Border Gateway Protocol (BGP) neighbor that does not support capability negotiation, use the **neighbor override-capability-neg** command in address family configuration mode. To disable the IPv6 address family for a BGP neighbor that does not support capability negotiation, use the **no** form of this command.

neighbor {*peer-group-name* | *ipv6-address*} **override-capability-neg**

no neighbor {*peer-group-name* | *ipv6-address*} **override-capability-neg**

Syntax Description

peer-group-name	Name of a BGP peer group.
ipv6-address	IPv6 address of the BGP neighbor. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

Command Default

Capability negotiation is enabled.

Command Modes

Address family configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Capability negotiation is used to establish a connection between BGP-speaking peers. If one of the BGP peers does not support capability negotiation, the connection is automatically terminated. The **neighbor override-capability-neg** command overrides the capability negotiation process and enables BGP-speaking peers to establish a connection.

The **neighbor override-capability-neg** command is supported only in address family configuration mode for the IPv6 address family.

Examples

The following example enables the IPv6 address family for BGP neighbor 7000::2:

```
Router(config)# address-family ipv6
Router(config-router-af)# neighbor 7000::2 override-capability-neg
```

The following example enables the IPv6 address family for all neighbors in the BGP peer group named group1:

```
Router(config)# address-family ipv6
Router(config-router-af)# neighbor group1 override-capability-neg
```

Related Commands

Command	Description
address-family ipv6	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard IPv6 address prefixes.

neighbor peer-group (assigning members)

To configure a BGP neighbor to be a member of a peer group, use the **neighbor peer-group** command in address family or router configuration mode. To remove the neighbor from the peer group, use the **no** form of this command.

neighbor {*ip-address* | *ipv6-address*} **peer-group** *peer-group-name*

no neighbor {*ip-address* | *ipv6-address*} **peer-group** *peer-group-name*

Syntax Description

ip-address	IP address of the BGP neighbor that belongs to the peer group specified by the *peer-group-name* argument.
ipv6-address	IPv6 address of the BGP neighbor that belongs to the peer group specified by the *peer-group-name* argument.
peer-group-name	Name of the BGP peer group to which this neighbor belongs.

Defaults

There are no BGP neighbors in a peer group.

Command Modes

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

Command History

Release	Modification
11.0	This command was introduced.
12.0(7)T	Address family configuration mode was added.
12.2(2)T	Support for IPv6 was added.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The neighbor at the IP address indicated inherits all the configured options of the peer group.

Note Using the **no** form of the **neighbor peer-group** command removes all of the BGP configuration for that neighbor, not just the peer group association.

Examples

The following router configuration mode example assigns three neighbors to the peer group named internal:

```
router bgp 100
 neighbor internal peer-group
 neighbor internal remote-as 100
 neighbor internal update-source loopback 0
 neighbor internal route-map set-med out
 neighbor internal filter-list 1 out
 neighbor internal filter-list 2 in
 neighbor 172.16.232.53 peer-group internal
 neighbor 172.16.232.54 peer-group internal
 neighbor 172.16.232.55 peer-group internal
 neighbor 172.16.232.55 filter-list 3 in
```

The following address family configuration mode example assigns three neighbors to the peer group named internal:

```
router bgp 100
address-family ipv4 unicast
 neighbor internal peer-group
 neighbor internal remote-as 100
 neighbor internal update-source loopback 0
 neighbor internal route-map set-med out
 neighbor internal filter-list 1 out
 neighbor internal filter-list 2 in
 neighbor 172.16.232.53 peer-group internal
 neighbor 172.16.232.54 peer-group internal
 neighbor 172.16.232.55 peer-group internal
 neighbor 172.16.232.55 filter-list 3 in
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
neighbor peer-group (creating)	Creates a BGP peer group.
neighbor shutdown	Disables a neighbor or peer group.

neighbor peer-group (creating)

To create a BGP or multiprotocol BGP peer group, use the **neighbor peer-group** command in address family or router configuration mode. To remove the peer group and all of its members, use the **no** form of this command.

neighbor *peer-group-name* **peer-group**

no neighbor *peer-group-name* **peer-group**

Syntax Description

peer-group-name	Name of the BGP peer group.

Defaults

There is no BGP peer group.

Command Modes

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

Command History

Release	Modification
11.0	This command was introduced.
11.1(20)CC	The **nlri unicast**, **nlri multicast**, and **nlri unicast multicast** keywords were added.
12.0(2)S	The **nlri unicast**, **nlri multicast**, and **nlri unicast multicast** keywords were added.
12.0(7)T	The **nlri unicast**, **nlri multicast**, and **nlri unicast multicast** keywords were removed. Address family configuration mode was added.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Often in a BGP or multiprotocol BGP speaker, many neighbors are configured with the same update policies (that is, same outbound route maps, distribute lists, filter lists, update source, and so on). Neighbors with the same update policies can be grouped into peer groups to simplify configuration and make update calculation more efficient.

Note Peer group members can span multiple logical IP subnets, and can transmit, or pass along, routes from one peer group member to another.

Once a peer group is created with the **neighbor peer-group** command, it can be configured with the **neighbor** commands. By default, members of the peer group inherit all the configuration options of the peer group. Members also can be configured to override the options that do not affect outbound updates.

All the peer group members will inherit the current configuration as well as changes made to the peer group. Peer group members will always inherit the following configuration options by default:

- remote-as (if configured)
- version
- update-source
- outbound route-maps
- outbound filter-lists
- outbound distribute-lists
- minimum-advertisement-interval
- next-hop-self

If a peer group is not configured with a remote-as option, the members can be configured with the **neighbor** {*ip-address* | *peer-group-name*} **remote-as** command. This command allows you to create peer groups containing external BGP (eBGP) neighbors.

Examples

The following example configurations show how to create these types of neighbor peer group:

- internal Border Gateway Protocol (iBGP) peer group
- eBGP peer group
- Multiprotocol BGP peer group

iBGP Peer Group

In the following example, the peer group named internal configures the members of the peer group to be iBGP neighbors. By definition, this is an iBGP peer group because the **router bgp** command and the **neighbor remote-as** command indicate the same autonomous system (in this case, autonomous system 100). All the peer group members use loopback 0 as the update source and use set-med as the outbound route map. The **neighbor internal filter-list 2 in** command shows that, except for 172.16.232.55, all the neighbors have filter list 2 as the inbound filter list.

```
router bgp 100
 neighbor internal peer-group
 neighbor internal remote-as 100
 neighbor internal update-source loopback 0
 neighbor internal route-map set-med out
 neighbor internal filter-list 1 out
 neighbor internal filter-list 2 in
 neighbor 172.16.232.53 peer-group internal
 neighbor 172.16.232.54 peer-group internal
 neighbor 172.16.232.55 peer-group internal
 neighbor 172.16.232.55 filter-list 3 in
```

eBGP Peer Group

The following example defines the peer group named external-peers without the **neighbor remote-as** command. By definition, this is an eBGP peer group because each individual member of the peer group is configured with its respective autonomous system number separately. Thus the peer group consists of

members from autonomous systems 200, 300, and 400. All the peer group members have the set-metric route map as an outbound route map and filter list 99 as an outbound filter list. Except for neighbor 172.16.232.110, all of them have 101 as the inbound filter list.

```
router bgp 100
 neighbor external-peers peer-group
 neighbor external-peers route-map set-metric out
 neighbor external-peers filter-list 99 out
 neighbor external-peers filter-list 101 in
 neighbor 172.16.232.90 remote-as 200
 neighbor 172.16.232.90 peer-group external-peers
 neighbor 172.16.232.100 remote-as 300
 neighbor 172.16.232.100 peer-group external-peers
 neighbor 172.16.232.110 remote-as 400
 neighbor 172.16.232.110 peer-group external-peers
 neighbor 172.16.232.110 filter-list 400 in
```

Multiprotocol BGP Peer Group

In the following example, all members of the peer group are multicast-capable:

```
router bgp 100
neighbor 10.1.1.1 remote-as 1
neighbor 172.16.2.2 remote-as 2
address-family ipv4 multicast
 neighbor mygroup peer-group
 neighbor 10.1.1.1 peer-group mygroup
 neighbor 172.16.2.2 peer-group mygroup
 neighbor 10.1.1.1 activate
 neighbor 172.16.2.2 activate
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
clear ip bgp peer-group	Removes all the members of a BGP peer group.
show ip bgp peer-group	Displays information about BGP peer groups.

neighbor remote-as

To add an entry to the BGP or multiprotocol BGP neighbor table, use the **neighbor remote-as** command in router configuration mode. To remove an entry from the table, use the **no** form of this command.

neighbor {*ip-address* | *ipv6-address*[**%**] | *peer-group-name*} **remote-as** *autonomous-system-number* [**alternate-as** *autonomous-system-number ...*]

no neighbor *{ip-address* | *ipv6-address*[**%**] | *peer-group-name*} **remote-as** *autonomous-system-number* [**alternate-as** *autonomous-system-number ...*]

Syntax Description

ip-address	IP address of the neighbor.
ipv6-address	IPv6 address of the neighbor.
%	(Optional) IPv6 link-local address identifier. This keyword needs to be added whenever a link-local IPv6 address is used outside the context of its interface.
peer-group-name	Name of a BGP peer group.
autonomous-system-number	Number of an autonomous system to which the neighbor belongs in the range from 1 to 65535. • In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, 4-byte autonomous system numbers are supported in the range from 65536 to 4294967295 in asplain notation and in the range from 1.0 to 65535.65535 in asdot notation. • In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, 4-byte autonomous system numbers are supported in the range from 1.0 to 65535.65535 in asdot notation only. For more details about autonomous system number formats, see the **router bgp** command. When used with the **alternate-as** keyword, up to five autonomous system numbers may be entered.
alternate-as	(Optional) Specifies an alternate autonomous system in which a potential dynamic neighbor can be identified. Up to five autonomous system numbers may be entered when this keyword is specified.

Command Default

There are no BGP or multiprotocol BGP neighbor peers.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
10.0	This command was introduced.
11.0	The *peer-group-name* argument was added.

Release	Modification
11.1(20)CC	The **nlri unicast**, **nlri multicast**, and **nlri unicast multicast** keywords were added.
12.0(7)T	The **nlri unicast**, **nlri multicast**, and **nlri unicast multicast** keywords were removed.
12.2(4)T	Support for the IPv6 address family was added.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was modified. The **%** keyword was added.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH. The **alternate-as** keyword was added to support BGP dynamic neighbors.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
12.0(32)S12	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(24)T	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.3	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SXI1	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
12.2(33)SRE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.

Usage Guidelines

Specifying a neighbor with an autonomous system number that matches the autonomous system number specified in the **router bgp** global configuration command identifies the neighbor as internal to the local autonomous system. Otherwise, the neighbor is considered external.

If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command.

By default, neighbors that are defined using the **neighbor remote-as** command in router configuration mode exchange only unicast address prefixes. To exchange other address prefix types, such as multicast and Virtual Private Network (VPN) Version 4, neighbors must also be activated in the appropriate address family configuration mode.

Use the **alternate-as** keyword introduced in Cisco IOS Release 12.2(33)SXH to specify up to five alternate autonomous systems in which a dynamic BGP neighbor may be identified. BGP dynamic neighbor support allows BGP peering to a group of remote neighbors that are defined by a range of IP addresses. BGP dynamic neighbors are configured using a range of IP addresses and BGP peer groups. After a subnet range is configured and associated with a BGP peer group using the **bgp listen** command and a TCP session is initiated for an IP address in the subnet range, a new BGP neighbor is dynamically created as a member of that group. The new BGP neighbor will inherit any configuration or templates for the group.

The **%** keyword is used whenever link-local IPv6 addresses are used outside the context of their interfaces. This keyword does not need to be used for non-link-local IPv6 addresses.

In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, the Cisco implementation of 4-byte autonomous system numbers uses asplain—65538 for example—as the default regular expression match and output display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain format and the asdot format as described in RFC 5396. To change the default regular expression match and output display of 4-byte autonomous system numbers to asdot format, use the **bgp asnotation dot** command followed by the **clear ip bgp *** command to perform a hard reset of all current BGP sessions.

In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, the Cisco implementation of 4-byte autonomous system numbers uses asdot—1.2 for example—as the only configuration format, regular expression match, and output display, with no asplain support.

Note In Cisco IOS releases that include 4-byte ASN support, command accounting and command authorization that include a 4-byte ASN number are sent in the asplain notation irrespective of the format that is used on the command-line interface.

To ensure a smooth transition, we recommend that all BGP speakers within an autonomous system that is identified using a 4-byte autonomous system number, be upgraded to support 4-byte autonomous system numbers.

Examples

The following example specifies that a router at the address 10.108.1.2 is an internal BGP (iBGP) neighbor in autonomous system number 65200:

```
router bgp 65200
 network 10.108.0.0
 neighbor 10.108.1.2 remote-as 65200
```

The following example specifies that a router at the IPv6 address 2001:0DB8:1:1000::72a is an external BGP (eBGP) neighbor in autonomous system number 65001:

```
router bgp 65300
 address-family ipv6 vrf site1
 neighbor 2001:0DB8:1:1000::72a remote-as 65001
```

The following example assigns a BGP router to autonomous system 65400, and two networks are listed as originating in the autonomous system. Then the addresses of three remote routers (and their autonomous systems) are listed. The router being configured will share information about networks 10.108.0.0 and 192.168.7.0 with the neighbor routers. The first router is a remote router in a different autonomous system from the router on which this configuration is entered (an eBGP neighbor); the second **neighbor remote-as** command shows an internal BGP neighbor (with the same autonomous

system number) at address 10.108.234.2; and the last **neighbor remote-as** command specifies a neighbor on a different network from the router on which this configuration is entered (also an eBGP neighbor).

```
router bgp 65400
 network 10.108.0.0
 network 192.168.7.0
 neighbor 10.108.200.1 remote-as 65200
 neighbor 10.108.234.2 remote-as 65400
 neighbor 172.29.64.19 remote-as 65300
```

The following example configures neighbor 10.108.1.1 in autonomous system 65001 to exchange only multicast routes:

```
router bgp 65001
 neighbor 10.108.1.1 remote-as 65001
 neighbor 172.31 1.2 remote-as 65001
 neighbor 172.16.2.2 remote-as 65002
 address-family ipv4 multicast
  neighbor 10.108.1.1 activate
  neighbor 172.31 1.2 activate
  neighbor 172.16.2.2 activate
  exit-address-family
```

The following example configures neighbor 10.108.1.1 in autonomous system 65001 to exchange only unicast routes:

```
router bgp 65001
 neighbor 10.108.1.1 remote-as 65001
 neighbor 172.31 1.2 remote-as 65001
 neighbor 172.16.2.2 remote-as 65002
```

The following example, configurable only in Cisco IOS Release 12.2(33)SXH and later releases, configures a subnet range of 192.168.0.0/16 and associates this listen range with a BGP peer group. Note that the listen range peer group that is configured for the BGP dynamic neighbor feature can be activated in the IPv4 address family using the **neighbor activate** command. After the initial configuration on Router 1, when Router 2 starts a BGP router session and adds Router 1 to its BGP neighbor table, a TCP session is initiated, and Router 1 creates a new BGP neighbor dynamically because the IP address of the new neighbor is within the listen range subnet.

Router 1

```
enable
configure terminal
router bgp 45000
 bgp log-neighbor-changes
 neighbor group192 peer-group
 bgp listen range 192.168.0.0/16 peer-group group192
 neighbor group192 remote-as 40000 alternate-as 50000
 address-family ipv4 unicast
 neighbor group192 activate
 end
```

Router 2

```
enable
configure terminal
router bgp 50000
 neighbor 192.168.3.1 remote-as 45000
 exit
```

If the **show ip bgp summary** command is now entered on Router 1, the output shows the dynamically created BGP neighbor, 192.168.3.2.

```
Router1# show ip bgp summary

BGP router identifier 192.168.3.1, local AS number 45000
BGP table version is 1, main routing table version 1

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
*192.168.3.2    4 50000       2       2        0    0    0 00:00:37        0
* Dynamically created based on a listen range command
Dynamically created neighbors: 1/(200 max), Subnet ranges: 1

BGP peergroup group192 listen range group members:
  192.168.0.0/16
```

The following example configures a BGP process for autonomous system 65538 and configures two external BGP neighbors in different autonomous systems using 4-byte autonomous system numbers in asplain format. This example is supported only on Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, or later releases.

```
router bgp 65538
 neighbor 192.168.1.2 remote-as 65536
 neighbor 192.168.3.2 remote-as 65550
 neighbor 192.168.3.2 description finance
 !
 address-family ipv4
  neighbor 192.168.1.2 activate
  neighbor 192.168.3.2 activate
  no auto-summary
  no synchronization
  network 172.17.1.0 mask 255.255.255.0
  exit-address-family
```

The following example configures a BGP process for autonomous system 1.2 and configures two external BGP neighbors in different autonomous systems using 4-byte autonomous system numbers in asdot format. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(32)S12, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, 12.4(24)T, Cisco IOS XE Release 2.3, or a later release.

```
router bgp 1.2
 neighbor 192.168.1.2 remote-as 1.0
 neighbor 192.168.3.2 remote-as 1.14
 neighbor 192.168.3.2 description finance
 !
 address-family ipv4
  neighbor 192.168.1.2 activate
  neighbor 192.168.3.2 activate
  no auto-summary
  no synchronization
  network 172.17.1.0 mask 255.255.255.0
  exit-address-family
```

Related Commands

Command	Description
bgp asnotation dot	Changes the default display and the regular expression match format of BGP 4-byte autonomous system numbers from asplain (decimal values) to dot notation.
bgp listen	Associates a subnet range with a BGP peer group and activates the BGP dynamic neighbors feature.

neighbor peer-group	Creates a BGP peer group.
router bgp	Configures the BGP routing process.

neighbor route-map

To apply a route map to incoming or outgoing routes, use the **neighbor route-map** command in address family or router configuration mode. To remove a route map, use the **no** form of this command.

neighbor {*ip-address* | *peer-group-name* | *ipv6-address* [**%**]} **route-map** *map-name* {**in** | **out**}

no neighbor {*ip-address* | *peer-group-name* | *ipv6-address* [**%**]} **route-map** *map-name* {**in** | **out**}

Syntax Description

ip-address	IP address of the neighbor.
peer-group-name	Name of a BGP or multiprotocol BGP peer group.
ipv6-address	IPv6 address of the neighbor.
%	(Optional) IPv6 link-local address identifier. This keyword needs to be added whenever a link-local IPv6 address is used outside the context of its interface.
map-name	Name of a route map.
in	Applies route map to incoming routes.
out	Applies route map to outgoing routes.

Command Default

No route maps are applied to a peer.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
10.0	This command was introduced.
12.0(7)T	Address family configuration mode was added.
12.2(4)T	Support for IPv6 was added.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	The **%** keyword was added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

When specified in address family configuration mode, this command applies a route map to that particular address family only. When specified in router configuration mode, this command applies a route map to IPv4 or IPv6 unicast routes only.

If an outbound route map is specified, it is proper behavior to only advertise routes that match at least one section of the route map.

If you specify a BGP or multiprotocol BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command. Specifying the command for a neighbor overrides the inbound policy that is inherited from the peer group.

The **%** keyword is used whenever link-local IPv6 addresses are used outside the context of their interfaces. This keyword does not need to be used for non-link-local IPv6 addresses.

Examples

The following router configuration mode example applies a route map named internal-map to a BGP incoming route from 172.16.70.24:

```
router bgp 5
 neighbor 172.16.70.24 route-map internal-map in

route-map internal-map
 match as-path 1
 set local-preference 100
```

The following address family configuration mode example applies a route map named internal-map to a multiprotocol BGP incoming route from 172.16.70.24:

```
router bgp 5
address-family ipv4 multicast
 neighbor 172.16.70.24 route-map internal-map in

route-map internal-map
 match as-path 1
 set local-preference 100
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IP Version 4 address prefixes.
address-family ipv6	Enters address family configuration mode for configuring routing sessions such as BGP that use standard IPv6 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPN Version 4 address prefixes.
address-family vpnv6	Places the router in address family configuration mode for configuring routing sessions that use standard VPNv6 address prefixes.
neighbor remote-as	Creates a BGP peer group.

neighbor route-reflector-client

To configure the router as a BGP route reflector and configure the specified neighbor as its client, use the **neighbor route-reflector-client** command in address family or router configuration mode. To indicate that the neighbor is not a client, use the **no** form of this command.

neighbor {*ip-address* | *ipv6-address* | *peer-group-name*} **route-reflector-client**

no neighbor {*ip-address* | *ipv6-address* | *peer-group-name*} **route-reflector-client**

Syntax Description

ip-address	IP address of the BGP neighbor being identified as a client.
ipv6-address	IPv6 address of the BGP neighbor being identified as a client.
peer-group-name	Name of a BGP peer group.

Command Default

There is no route reflector in the autonomous system.

Command Modes

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

Command History

Release	Modification
11.1	This command was introduced.
12.0(7)T	Address family configuration mode was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	The *ipv6-address* and *peer-group-name* arguments were added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 3.1S	This command was updated. It was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

By default, all internal BGP (iBGP) speakers in an autonomous system must be fully meshed, and neighbors do not readvertise iBGP learned routes to neighbors, thus preventing a routing information loop. When all the clients are disabled, the local router is no longer a route reflector.

If you use route reflectors, all iBGP speakers need not be fully meshed. In the route reflector model, an Interior BGP peer is configured to be a *route reflector* responsible for passing iBGP learned routes to iBGP neighbors. This scheme eliminates the need for each router to talk to every other router.

Use the **neighbor route-reflector-client** command to configure the local router as the route reflector and the specified neighbor as one of its clients. All the neighbors configured with this command will be members of the client group and the remaining iBGP peers will be members of the nonclient group for the local route reflector.

The **bgp client-to-client reflection** command controls client-to-client reflection.

Examples

In the following router configuration mode example, the local router is a route reflector. It passes learned iBGP routes to the neighbor at 172.16.70.24.

```
router bgp 5
 neighbor 172.16.70.24 route-reflector-client
```

In the following address family configuration mode example, the local router is a route reflector. It passes learned iBGP routes to the neighbor at 172.16.70.24.

```
router bgp 5
address-family ipv4 unicast
 neighbor 172.16.70.24 route-reflector-client
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IP Version 4 address prefixes.
address-family ipv6	Enters address family configuration mode for configuring routing sessions such as BGP that use standard IPv6 address prefixes.
address-family vpnv6	Places the router in address family configuration mode for configuring routing sessions such as BGP that use standard VPNv6 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPN Version 4 address prefixes.
address-family vpnv6	Places the router in address family configuration mode for configuring routing sessions such as BGP that use standard VPNv6 address prefixes.
bgp client-to-client reflection	Restores route reflection from a BGP route reflector to clients.
bgp cluster-id	Configures the cluster ID if the BGP cluster has more than one route reflector.
neighbor route-reflector-client	Configures the router as a BGP route reflector and configures the specified neighbor as its client.
show bgp ipv6	Displays entries in the IPv6 BGP routing table.
show ip bgp	Displays entries in the BGP routing table.

neighbor send-community

To specify that a communities attribute should be sent to a BGP neighbor, use the **neighbor send-community** command in address family or router configuration mode. To remove the entry, use the **no** form of this command.

neighbor {*ip-address* | *ipv6-address* | *peer-group-name*} **send-community** [**both** | **standard** | **extended**]

no neighbor {*ip-address* | *ipv6-address* | *peer-group-name*} **send-community**

Syntax Description

ip-address	IP address of the neighbor.
ipv6-address	IPv6 address of the neighbor.
peer-group-name	Name of a BGP peer group.
both	(Optional) Specifies that both standard and extended communities will be sent.
standard	(Optional) Specifies that only standard communities will be sent.
extended	(Optional) Specifies that only extended communities will be sent.

Command Default

No communities attribute is sent to any neighbor.

Command Modes

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

Command History

Release	Modification
10.3	This command was introduced.
11.0	The *peer-group-name* argument was added.
12.0(7)T	Address family configuration mode was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	The *ipv6-address* argument was added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command.

Examples

In the following router configuration mode example, the router belongs to autonomous system 109 and is configured to send the communities attribute to its neighbor at IP address 172.16.70.23:

```
router bgp 109
 neighbor 172.16.70.23 send-community
```

In the following address family configuration mode example, the router belongs to autonomous system 109 and is configured to send the communities attribute to its neighbor at IP address 172.16.70.23:

```
router bgp 109
address-family ipv4 multicast
 neighbor 172.16.70.23 send-community
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IP Version 4 address prefixes.
address-family ipv6	Places the router in address family configuration mode for configuring routing sessions such as BGP that use standard IPv6 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPN Version 4 address prefixes.
address-family vpnv6	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard VPNv6 address prefixes.
match community	Matches a BGP community.
neighbor remote-as	Creates a BGP peer group.
set community	Sets the BGP communities attribute.

neighbor send-label

To enable a Border Gateway Protocol (BGP) router to send Multiprotocol Label Switching (MPLS) labels with BGP routes to a neighboring BGP router, use the **neighbor send-label** command in address family configuration mode or router configuration mode. To disable this feature, use the **no** form of this command.

neighbor {*ip-address* | *ipv6-address* | *peer-group-name*} **send-label** [**explicit-null**]

neighbor {*ip-address* | *ipv6-address* | *peer-group-name*} **send-label** [**explicit-null**]

Syntax Description

ip-address	IP address of the neighboring router.
ipv6-address	IPv6 address of the neighboring router.
peer-group-name	Name of a BGP peer group.
send-label	Sends Network Layer Reachability Information (NLRI) and MPLS labels to this peer.
explicit-null	(Optional) Advertises the Explicit Null label.

Command Default

BGP routers distribute only BGP routes.

Command Modes

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

Command History

Release	Modification
12.0(21)ST	This command was introduced.
12.0(22)S	This command was modified. The *ipv6-address* argument was added.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

The **neighbor send-label** command enables a router to use BGP to distribute MPLS labels along with IPv4 routes to a peer router. You must issue this command on both the local and the neighboring router.

This command has the following restrictions:

- If a BGP session is running when you issue the **neighbor send-label** command, the BGP session flaps immediately after the command is issued.

- In router configuration mode, only IPv4 addresses are distributed.

Use the **neighbor send-label** command in address family configuration mode, to bind and advertise IPv6 prefix MPLS labels. Using this command in conjunction with the **mpls ipv6 source-interface** global configuration command allows IPv6 traffic to run over an IPv4 MPLS network without any software or hardware configuration changes in the backbone. Edge routers configured to run both IPv4 and IPv6 traffic forward IPv6 traffic using MPLS and multiprotocol internal BGP (MP-iBGP).

Cisco IOS software installs /32 routes for directly connected external BGP (eBGP) peers when the BGP session for such a peer comes up. The /32 routes are installed only when MPLS labels are exchanged between such peers. Directly connected eBGP peers exchange MPLS labels for:

- IP address families (IPv4 and IPv6) with the **neighbor send-label** command enabled for the peers
- VPN address families (VPNv4 and VPNv6)

A single BGP session can include multiple address families. If one of the families exchanges MPLS labels, the /32 neighbor route is installed for the connected peer.

Examples

The following example shows how to enable a router in autonomous system 65000 to send MPLS labels with BGP routes to the neighboring BGP router at 192.168.0.1:

```
Router(config)# router bgp 65000
Router(config-router)# neighbor 192.168.0.1 remote-as 65001
Router(config-router)# neighbor 192.168.0.1 send-label
```

The following example shows how to enable a router in the autonomous system 65000 to bind and advertise IPv6 prefix MPLS labels and send the labels with BGP routes to the neighboring BGP router at 192.168.99.70:

```
Router(config)# router bgp 65000
Router(config-router)# neighbor 192.168.99.70 remote-as 65000
Router(config-router)# address-family ipv6
Router(config-router-af)# neighbor 192.168.99.70 activate
Router(config-router-af)# neighbor 192.168.99.70 send-label
```

Related Commands

Command	Description
address-family ipv6	Enters address family configuration mode for configuring routing sessions such as BGP that use standard IPv6 address prefixes.
neighbor activate	Enables the exchange of information with a neighboring router.
neighbor remote-as	Adds an entry to the BGP or multiprotocol BGP neighbor table.
mpls ipv6 source-interface	Specifies an IPv6 address of an interface to be used as the source address for locally generated IPv6 packets to be sent over an MPLS network.

neighbor translate-update

To generate multiprotocol IPv6 Border Gateway Protocol (BGP) updates that correspond to unicast IPv6 updates received from a peer, use the **neighbor translate-update** command in address family or router configuration mode. To return to default values, use the **no** form of the command.

neighbor *ipv6-address* **translate-update ipv6 multicast** [**unicast**]

no neighbor *ipv6-address* **translate-update ipv6 multicast** [**unicast**]

Syntax Description

ipv6-address	Resets the TCP connection to the specified IPv6 BGP neighbor and removes all routes learned from the connection from the BGP table. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
IPv6 multicast	Specifies IPv6 multicast address prefixes.
unicast	(Optional) Specifies IPv6 unicast address prefixes.

Command Default

No BGP updates for unicast IPv6 are updated

Command Modes

Address family configuration
Router configuration

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The multicast BGP (MBGP) translate-update feature generally is used in an MBGP-capable router that peers with a customer site that has a router that is only BGP capable; the customer site has not or cannot upgrade the router to an MBGP-capable image. Because the customer site cannot originate MBGP advertisements, the router with which it peers will translate the BGP prefixes into MBGP prefixes, which are used for multicast-source Reverse Path Forwarding (RPF) lookup.

Examples

The following example generates multiprotocol IPv6 BGP updates that correspond to unicast IPv6 updates received from peer at address 7000::2:

```
neighbor 7000::2 translate-update ipv6 multicast
```

neighbor update-source

To have the Cisco IOS software allow Border Gateway Protocol (BGP) sessions to use any operational interface for TCP connections, use the **neighbor update-source** command in router configuration mode. To restore the interface assignment to the closest interface, which is called the best local address, use the **no** form of this command.

neighbor {*ip-address* | *ipv6-address*[**%**] | *peer-group-name*} **update-source** *interface-type interface-number*

no neighbor {*ip-address* | *ipv6-address*[**%**] | *peer-group-name*} **update-source** *interface-type interface-number*

Syntax Description

ip-address	IPv4 address of the BGP-speaking neighbor.
ipv6-address	IPv6 address of the BGP-speaking neighbor.
%	(Optional) IPv6 link-local address identifier. This keyword needs to be added whenever a link-local IPv6 address is used outside the context of its interface.
peer-group-name	Name of a BGP peer group.
interface-type	Interface type.
interface-number	Interface number.

Command Default

Best local address

Command Modes

Router configuration (config-router)

Command History

Release	Modification
10.0	This command was introduced.
12.2(4)T	The *ipv6-address* argument was added.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	The **%** keyword was added.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 series routers.

Usage Guidelines

This command can work in conjunction with the loopback interface feature described in the "Interface Configuration Overview" chapter of the *Cisco IOS Interface and Hardware Component Configuration Guide*.

If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command.

The **neighbor update-source** command must be used to enable IPv6 link-local peering for internal or external BGP sessions.

The **%** keyword is used whenever link-local IPv6 addresses are used outside the context of their interfaces and for these link-local IPv6 addresses you must specify the interface they are on. The syntax becomes <IPv6 local-link address>%<interface name>, for example, FE80::1%Ethernet1/0. Note that the interface type and number must not contain any spaces, and be used in full-length form because name shortening is not supported in this situation. The % keyword and subsequent interface syntax is not used for non-link-local IPv6 addresses.

Examples

The following example sources BGP TCP connections for the specified neighbor with the IP address of the loopback interface rather than the best local address:

```
router bgp 65000
 network 172.16.0.0
 neighbor 172.16.2.3 remote-as 110
 neighbor 172.16.2.3 update-source Loopback0
```

The following example sources IPv6 BGP TCP connections for the specified neighbor in autonomous system 65000 with the global IPv6 address of loopback interface 0 and the specified neighbor in autonomous system 65400 with the link-local IPv6 address of Fast Ethernet interface 0/0. Note that the link-local IPv6 address of FE80::2 is on Ethernet interface 1/0.

```
router bgp 65000
 neighbor 3ffe::3 remote-as 65000
 neighbor 3ffe::3 update-source Loopback0
 neighbor fe80::2%Ethernet1/0 remote-as 65400
 neighbor fe80::2%Ethernet1/0 update-source FastEthernet 0/0
 address-family ipv6
  neighbor 3ffe::3 activate
  neighbor fe80::2%Ethernet1/0 activate
  exit-address-family
```

Related Commands

Command	Description
neighbor activate	Enables the exchange of information with a BGP neighboring router.
neighbor remote-as	Adds an entry to the BGP or multiprotocol BGP neighbor table.

network (BGP and multiprotocol BGP)

To specify the networks to be advertised by the Border Gateway Protocol (BGP) and multiprotocol BGP routing processes, use the **network** command in address family or router configuration mode. To remove an entry from the routing table, use the **no** form of this command.

network {*network-number* [**mask** *network-mask*] | *nsap-prefix*} [**route-map** *map-tag*]

no network {*network-number* [**mask** *network-mask*] | *nsap-prefix*} [**route-map** *map-tag*]

Syntax Description

network-number	Network that BGP or multiprotocol BGP will advertise.
mask *network-mask*	(Optional) Network or subnetwork mask with mask address.
nsap-prefix	Network service access point (NSAP) prefix of the Connectionless Network Service (CLNS) network that BGP or multiprotocol BGP will advertise. This argument is used only under NSAP address family configuration mode.
route-map *map-tag*	(Optional) Identifier of a configured route map. The route map should be examined to filter the networks to be advertised. If not specified, all networks are advertised. If the keyword is specified, but no route map tags are listed, no networks will be advertised.

Command Default

No networks are specified.

Command Modes

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

Command History

Release	Modification
10.0	This command was introduced.
12.0	The limit of 200 network commands per BGP router was removed.
11.1(20)CC	The **nlri unicast**, **nlri multicast**, and **nlri unicast multicast** keywords were added.
12.0(7)T	The **nlri unicast**, **nlri multicast**, and **nlri unicast multicast** keywords were removed. Address family configuration mode was added.
12.2(8)T	The *nsap-prefix* argument was added to address family configuration mode.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

BGP and multiprotocol BGP networks can be learned from connected routes, from dynamic routing, and from static route sources.

The maximum number of **network** commands you can use is determined by the resources of the router, such as the configured NVRAM or RAM.

Examples

The following example sets up network 10.108.0.0 to be included in the BGP updates:

```
router bgp 65100
 network 10.108.0.0
```

The following example sets up network 10.108.0.0 to be included in the multiprotocol BGP updates:

```
router bgp 64800
address family ipv4 multicast
 network 10.108.0.0
```

The following example advertises NSAP prefix 49.6001 in the multiprotocol BGP updates:

```
router bgp 64500
 address-family nsap
  network 49.6001
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Enters the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IP Version 4 address prefixes.
address-family vpnv4	Enters the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
default-information originate (BGP)	Allows the redistribution of network 0.0.0.0 into BGP.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another.
router bgp	Configures the BGP routing process.

network (IPv6)

To configure the network source of the next hop to be used by the PE VPN, use the **network** command in router configuration mode. To disable the source, use the **no** form of this command.

network *ipv6-address*/*prefix-length*

no network *ipv6-address*/*prefix-length*

Syntax Description

ipv6-address	The IPv6 address to be used.
/*prefix-length*	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

Command Default

Next-hop network sources are not configured.

Command Modes

Address family configuration
Router configuration

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 3.1S	This command was updated. It was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

The *ipv6-address* argument in this command configures the IPv6 network number.

Examples

The following example places the router in address family configuration mode and configures the network source to be used as the next hop:

```
Router(config)# router bgp 100
Router(config-router)# network 2001:DB8:100::1/128
```

Related Commands

Command	Description
address-family ipv6	Enters address family configuration mode for configuring routing sessions such as BGP that use standard IPv6 address prefixes.
address-family vpnv6	Places the router in address family configuration mode for configuring routing sessions that use standard VPNv6 address prefixes.

nis address

To specify the network information service (NIS) address of an IPv6 server to be sent to the client, use the **nis address** command in DHCP for IPv6 pool configuration mode. To remove the NIS address, use the **no** form of this command.

nis address *ipv6-address*

no nis address *ipv6-address*

Syntax Description

ipv6-address	The NIS address of an IPv6 server to be sent to the client.

Command Default

No NIS address is specified.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

The Dynamic Host Configuration Protocol (DHCP) for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The NIS server option provides a list of one or more IPv6 addresses of NIS servers available to send to the client. The client must view the list of NIS servers as an ordered list, and the server may list the NIS servers in the order of the server's preference.

The NIS server option code is 27. For more information on DHCP options and suboptions, see the "DHCPv6 Options" appendix in the *Network Registrar User's Guide*, Release 6.2.

Examples

The following example shows how to specify the NIS address of an IPv6 server:

```
nis address 23::1
```

Related Commands

Command	Description
import nis address	Imports the NIS server option to a DHCP for IPv6 client.
nis domain-name	Enables a server to convey a client's NIS domain name information to the client.

nis domain-name

To enable a server to convey a client's network information service (NIS) domain name information to the client, use the **nis domain-name** command in DHCP for IPv6 pool configuration mode. To remove the domain name, use the **no** form of this command.

nis domain-name *domain-name*

no nis domain-name *domain-name*

Syntax Description

domain-name	The domain name of an IPv6 server to be sent to the client.

Command Default

No NIS domain name is specified.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

The Dynamic Host Configuration Protocol (DHCP) for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The NIS domain name option provides a NIS domain name for the client. Use the **nis domain-name** command to specify the client's NIS domain name that the server sends to the client.

The NIS domain name option code is 29. For more information on DHCP options and suboptions, see the "DHCPv6 Options" appendix in the *Network Registrar User's Guide*, Release 6.2.

Examples

The following example shows how to enable the IPv6 server to specify the NIS domain name of a client:

```
nis domain-name cisco1.com
```

Related Commands

Command	Description
import nis domain	Imports the NIS domain name option to a DHCP for IPv6 client.
nis address	Specifies the NIS address of an IPv6 server to be sent to the client.

nisp address

To specify the network information service plus (NIS+) address of an IPv6 server to be sent to the client, use the **nisp address** command in DHCP for IPv6 pool configuration mode. To remove the NIS+ address, use the **no** form of the command.

nisp address *ipv6-address*

no nisp address *ipv6-address*

Syntax Description

ipv6-address	The NIS+ address of an IPv6 server to be sent to the client.

Command Default

No NIS+ address is specified.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

The Dynamic Host Configuration Protocol (DHCP) for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The NIS+ servers option provides a list of one or more IPv6 addresses of NIS+ servers available to send to the client. The client must view the list of NIS+ servers as an ordered list, and the server may list the NIS+ servers in the order of the server's preference.

The NIS+ servers option code is 28. For more information on DHCP options and suboptions, see the "DHCPv6 Options" appendix in the *Network Registrar User's Guide*, Release 6.2.

Examples

The following example shows how to specify the NIS+ address of an IPv6 server:

```
nisp address 33::1
```

Related Commands

Command	Description
import nisp address	Imports the NIS+ servers option to a DHCP for IPv6 client.
nisp domain-name	Enables a server to convey a client's NIS+ domain name information to the client.

nisp domain-name

To enable an IPv6 server to convey a client's network information service plus (NIS+) domain name information to the client, use the **nisp domain-name** command in DHCP for IPv6 pool configuration mode. To remove the domain name, use the **no** form of this command.

nisp domain-name *domain-name*

no nisp domain-name *domain-name*

Syntax Description

domain-name	The NIS+ domain name of an IPv6 server to be sent to the client.

Command Default

No NIS+ domain name is specified.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

The Dynamic Host Configuration Protocol (DHCP) for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The NIS+ domain name option provides a NIS+ domain name for the client. Use the **nisp domain-name** command to enable a server to send the client its NIS+ domain name information.

The NIS+ domain name option code is 30. For more information on DHCP options and suboptions, see the "DHCPv6 Options" appendix in the *Network Registrar User's Guide*, Release 6.2.

Examples

The following example shows how to enable the IPv6 server to specify the NIS+ domain name of a client:

```
nisp domain-name cisco1.com
```

Related Commands

Command	Description
import nisp domain	Imports the NIS+ domain name option to a DHCP for IPv6 client.
nisp address	Specifies the NIS+ address of an IPv6 server to be sent to the client.

ntp access-group

To control access to the Network Time Protocol (NTP) services on the system, use the **ntp access-group** command in global configuration mode. To remove access control to the NTP services, use the **no** form of this command.

ntp access-group {**peer** | **query-only** | **serve** | **serve-only**} {*access-list-number* | *access-list-number-expanded* | *access-list-name*} [**kod**]

no ntp [**access-group** {**peer** | **query-only** | **serve** | **serve-only**} {*access-list-number* | *access-list-number-expanded* | *access-list-name*}]

Syntax Description

peer	Allows time requests and NTP control queries and allows the system to synchronize to the remote system.
query-only	Allows only NTP control queries. See RFC 1305 (NTP version 3).
serve	Allows time requests and NTP control queries, but does not allow the system to synchronize to the remote system.
serve-only	Allows only time requests. **Note** You must configure the **ntp server** *ip-address* command before using the **serve-only** keyword.
access-list-number	Number (from 1 to 99) of a standard IPv4 access list.
access-list-number-expanded	Number (from 1300 to 1999) of an expanded range IPv4 access list.
access-list-name	Name of an access list.
kod	(Optional) Sends the "Kiss-o-Death" (KOD) packet to any host that tries to send a packet that is not compliant with the access-group policy.

Command Default

By default, there is no access control. Full access is granted to all systems.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.4(15)T	This command was modified in a release earlier than Cisco IOS Release 12.4(15)T. The *access-list-number-expanded* argument was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was modified. The *access-list-name* argument and **kod** keyword were added. Support for IPv6 was added.

Release	Modification
12.2(33)SXJ	This command was modified. The *access-list-name* argument and **kod** keyword were added. Support for IPv6 was added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

The access group options are scanned in the following order from the least restrictive to most restrictive:

1. **peer**
2. **query-only**
3. **serve**
4. **serve-only**

Access is granted for the first match that is found. If no access groups are specified, all access is granted to all sources. If you specify any access groups, only the specified access is granted. This facility provides minimal security for the time services of the system. However, it can be circumvented by a determined programmer. If tighter security is desired, use the NTP authentication facility.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp access-group** command, the NTP service is activated (if it has not already been activated) and access control to NTP services is configured simultaneously.

When you enter the **no ntp access-group** command, only access control to NTP services is removed. The NTP service itself remains active, along with any other previously configured NTP functions.

To disable the NTP service on a device, use the **no ntp** command without any keywords in global configuration mode. For example, if you want to remove not only the access control to NTP services, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

Examples

The following example shows how to configure a system to allow itself to be synchronized by a peer from access list 99. However, the system restricts access to allow only time requests from access list 42.

```
Router(config)# ntp access-group peer 99
Router(config)# ntp access-group serve-only 42
```

In the following IPv6 example, a KOD packet is sent to any host that tries to send a packet that is not compliant with the access-group policy:

```
Router(config)# ntp access-group serve acl1 kod
```

The following example shows how to remove all the configured NTP options and disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
access-list	Configures the access list mechanism for filtering frames by protocol type or vendor code.
ntp server	Allows the software clock to be synchronized by a time server.

ntp authenticate

To enable Network Time Protocol (NTP) authentication, use the **ntp authenticate** command in global configuration mode. To disable the function, use the **no** form of this command.

ntp authenticate

no ntp [**authenticate**]

Syntax Description

This command has no arguments or keywords.

Command Default

By default, NTP authentication is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was modified. Support for NTPv4 and IPv6 was added.
12.2(33)SXJ	This command was modified. Support for NTPv4 and IPv6 was added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

Use this command if you want to authenticate NTP. If this command is specified, the system will not synchronize to another system unless it carries one of the authentication keys specified in the **ntp trusted-key** global configuration command.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp authenticate** command, the NTP service is activated (if it has not already been activated) and NTP authentication is enabled simultaneously.

In the **no** form of any **ntp** command, all the keywords are optional. When you enter the **no ntp authenticate** command, only the NTP authentication is removed from the NTP service. The NTP service itself remains active, along with any other functions you that previously configured.

To disable the NTP service on a device, you must enter the **no ntp** command without any keywords in global configuration mode. For example, if you previously issued the **ntp authenticate** command and you now want to disable not only the authentication, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

Examples

The following example shows how to configure the system to synchronize only to systems that provide the authentication key 42 in their NTP packets:

```
Router(config)# ntp authenticate
Router(config)# ntp authentication-key 42 md5 aNiceKey
Router(config)# ntp trusted-key 42
```

The following example shows how to remove all the configured NTP options and disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
ntp authentication-key	Defines an authentication key for NTP.
ntp trusted-key	Authenticates the identity of a system to which NTP will synchronize.

ntp authentication-key

To define an authentication key for Network Time Protocol (NTP), use the **ntp authentication-key** command in global configuration mode. To remove the authentication key for NTP, use the **no** form of this command.

ntp authentication-key *number* **md5** *key* [*encryption-type*]

no ntp [**authentication-key** *number*]

Syntax Description

number	Key number from 1 to 4294967295.
md5	Specifies the authentication key. Message authentication support is provided using the message digest 5 (MD5) algorithm. The key type **md5** is the only key type supported.
key	Character string of up to 32 characters that is the value of the MD5 key. **Note** In auto secure mode, an error is displayed on the console and the authentication key is not configured if the character string length exceeds 32.
encryption-type	(Optional) Authentication key encryption type. Range: 0 to 4294967295.

Command Default

No authentication key is defined for NTP.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was modified. Support for NTPv4 and IPv6 was added.
12.2(33)SXJ	This command was modified. Support for NTPv4 and IPv6 was added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

Use this command to define authentication keys for use with other NTP commands in order to provide a higher degree of security.

Note When this command is written to NVRAM, the key is encrypted so that it is not displayed in the configuration.

When you configure the authentication key using the **ntp authentication-key** command or using the **auto secure ntp** command, if the length of the MD5 key exceeds 32 characters, an error message is displayed.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp authentication-key** command, the NTP service is activated (if it has not already been activated) and the NTP authentication key is defined simultaneously.

When you enter the **no ntp authentication-key** command, only the NTP authentication key is removed from the NTP service. The NTP service itself remains active, along with any other previously configured NTP functions.

Note If a specific authentication key configuration is removed, the NTP process is not stopped until all the authentication key configurations are removed.

To disable the NTP service on a device, use the **no ntp** command without any keywords in global configuration mode. For example, if you want to remove not only the access control to NTP services, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

Examples

The following example shows how to configure the system to synchronize only to systems providing the authentication key 42 in their NTP packets:

```
Router(config)# ntp authenticate
Router(config)# ntp authentication-key 42 md5 aNiceKey
Router(config)# ntp trusted-key 42
```

The following example shows how to remove all the configured NTP options and disable the NTP server:

```
Router(config)# no ntp
```

The following example shows the error message displayed when the authentication key character string length exceeds 32:

```
Router(config)# ntp authentication-key 23 md5 11111111111111111111111111111111
%NTP: Key too long
```

Related Commands

Command	Description
auto secure	Secures the management and forwarding planes of the router.
ntp authenticate	Enables NTP authentication.
ntp peer	Configures the software clock to synchronize a peer or to be synchronized by a peer.
ntp server	Allows the software clock to be synchronized by a time server.
ntp trusted-key	Authenticates the identity of a system to which NTP will synchronize.

ntp broadcast client

To configure a device to receive Network Time Protocol (NTP) broadcast messages on a specified interface, use the **ntp broadcast client** command in interface configuration mode. To disable this capability, use the **no** form of this command.

ntp broadcast client [**novolley**]

no ntp [**broadcast** [**client**]]

Syntax Description

novolley	(Optional) Disables any messages sent to the broadcast server. Avoids the propagation delay measurement phase and directly uses a preconfigured value instead when used in conjunction with the **ntp broadcastdelay** command. **Note** Public key authentication does not work without the volley.

Command Default

By default, an interface is not configured to receive NTP broadcast messages.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was modified. Support for NTPv4 and IPv6 was added. The **novolley** keyword was added.
12.2(33)SXJ	This command was modified. Support for NTPv4 and IPv6 was added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

Use this command to allow the system to listen to broadcast packets on an interface-by-interface basis.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp broadcast client** command, the NTP service is activated (if it has not already been activated) and the device is configured to receive NTP broadcast packets on a specified interface simultaneously.

In the **no** form of any **ntp** command, all the keywords are optional. When you enter the **no ntp broadcast client** command, only the broadcast client configuration is removed from the NTP service. The NTP service itself remains active, along with any other functions that you previously configured.

To disable the NTP service on a device, you must enter the **no ntp** command without any keywords. For example, if you previously issued the **ntp broadcast client** command and you now want to remove not only the broadcast client capability, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

In IPv6 configuration, the **ntp broadcastdelay** command is used when the **ntp broadcast client** or **ntp multicast client** command is configured with the **novolley** keyword.

Examples

In the following example, the system is configured to receive (listen to) NTP broadcasts on Ethernet interface 1:

```
Router(config)# interface ethernet 1
Router(config-if)# ntp broadcast client
```

The following example shows how to remove all the configured NTP options and disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
ntp broadcastdelay	Sets the estimated round-trip delay between the system and an NTP broadcast server.
ntp multicast client	Configures the system to receive NTP multicast packets on a specified interface.

ntp broadcastdelay

To set the estimated round-trip delay between the Cisco IOS software and a Network Time Protocol (NTP) broadcast server, use the **ntp broadcastdelay** command in global configuration mode. To revert to the default value, use the **no** form of this command.

ntp broadcastdelay *microseconds*

no ntp [**broadcastdelay**]

Syntax Description

microseconds	Estimated round-trip time (in microseconds) for NTP broadcasts. The range is from 1 to 999999.

Command Default

By default, the round-trip delay between the Cisco IOS software and an NTP broadcast server is 3000 microseconds.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was modified. Support for NTPv4 and IPv6 was added.
12.2(33)SXJ	This command was modified. Support for NTPv4 and IPv6 was added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

Use the **ntp broadcastdelay** command when the router is configured as a broadcast client and the round-trip delay on the network is other than 3000 microseconds. In IPv6, the value set by this command should be used only when the **ntp broadcast client** and **ntp multicast client** commands have the **novolley** keyword enabled.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp broadcastdelay** command, the NTP service is activated (if it has not already been activated) and the estimated round-trip delay between the Cisco IOS software and an NTP broadcast server is set simultaneously.

In the **no** form of any **ntp** command, all the keywords are optional. When you enter the **no ntp broadcastdelay** command, only the estimated round-trip delay between the Cisco IOS software and an NTP broadcast server is removed from the NTP service. The NTP service itself remains active, along with any other functions you previously configured.

To disable the NTP service on a device, you must enter the **no ntp** command without any keywords in global configuration mode. For example, if you previously issued the **ntp broadcastdelay** command and you now want to remove not only the delay setting, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

Examples

The following example shows how to set the estimated round-trip delay between a router and the broadcast client to 5000 microseconds:

```
Router(config)# ntp broadcastdelay 5000
```

The following example shows how to remove all the configured NTP options and disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
ntp broadcast client	Configures the specified interface to receive NTP broadcast packets.
ntp multicast client	Configures the system to receive NTP multicast packets on a specified interface.

ntp disable

To prevent an interface from receiving Network Time Protocol (NTP) packets, use the **ntp disable** command in interface configuration mode. To enable the receipt of NTP packets on an interface, use the **no** form of this command.

ntp disable [**ip** | **ipv6**]

no ntp disable [**ip** | **ipv6**]

Syntax Description

ip	(Optional) Disables IP-based NTP traffic.
ipv6	(Optional) Disables IPv6-based NTP traffic.

Command Default

By default, interfaces receive NTP packets.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was modified. Support for IPv6 was added. The optional **ip** and **ipv6** keywords were added.
12.2(33)SXJ	This command was modified. Support for IPv6 was added. The optional **ip** and **ipv6** keywords were added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

This command provides a simple method of access control.

Use the **ntp disable** command in interface configuration mode to configure an interface to reject NTP packets. If the **ntp disable** command is configured on an interface that does not have any NTP service running, the interface remains disabled even after the NTP service is started by another NTP configuration. When you use the **ntp disable** command without the **ip** or **ipv6** keyword, NTP is disabled on the interface for all the address families.

When you enter the **no ntp disable** command in interface configuration mode, the interface that was configured to reject NTP packets is enabled to receive NTP packets.

Note Remove all NTP commands from an interface before entering the **ntp disable** command on that interface.

Configuring the **ntp disable** command on an interface does not stop the NTP service. To disable the NTP service on a device, use the **no ntp** command without keywords in global configuration mode. For example, if you had previously issued the **ntp disable** command and you now want to remove not only this restriction, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

Examples

The following example shows how to prevent Ethernet interface 0 from receiving NTP packets:

```
Router(config)# interface ethernet 0
Router(config-if)# ntp disable
```

The following example shows the message displayed when you try to execute the **ntp disable** command on an interface that has other NTP commands configured on it:

```
Router(config-if)# ntp disable

%NTP: Unconfigure other NTP commands on this interface before executing 'ntp disable'
```

If you had previously issued the **ntp disable** command and you now want to remove not only this restriction, but also all NTP functions from the device, use the **no ntp** command without keywords in global configuration mode. The following example shows how to disable the NTP service on a device:

```
Router(config)# no ntp
```

Related Commands

Command	Description
ntp	Activates the NTP service.

ntp clear drift

To reset the drift value stored in the persistent data file, use the **ntp clear drift** command in privileged EXEC mode.

ntp clear drift

Syntax Description

This command has no arguments or keywords.

Command Default

The drift value stored in the persistent data file is not reset.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SXJ	This command was integrated into Cisco IOS Release 12.2(33)SXJ.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

The **ntp clear drift** command is used to reset the local clock drift value in the persistent data file. The drift is the frequency offset between the local clock hardware and the authoritative time from the Network Time Protocol version 4 (NTPv4) servers. NTPv4 automatically computes this drift and uses it to compensate permanently for local clock imperfections.

This command is available only when the NTP service is activated using any **ntp** command in global configuration mode.

Examples

The following example shows how to reset the drift value in the persistent data file:

```
Router# ntp clear drift
```

Related Commands

Command	Description
ntp	Activates the NTP service.

ntp logging

To enable Network Time Protocol (NTP) message logging, use the **ntp logging** command in global configuration mode. To disable NTP logging, use the **no** form of this command.

ntp logging

no ntp [**logging**]

Syntax Description

This command has no arguments or keywords.

Command Default

NTP message logging is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was modified. Support for IPv6 was added.
12.2(33)SXJ	This command was modified. Support for IPv6 was added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

Use the **ntp logging** command to control the display of NTP logging messages.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp logging** command, the NTP service is activated (if it has not already been activated) and message logging is enabled simultaneously.

In the **no** form of any **ntp** command, all the keywords are optional. When you enter the **no ntp logging** command, only message logging is disabled in the NTP service. The NTP service itself remains active, along with any other functions that you previously configured.

To disable the NTP service on a device, you must enter the **no ntp** command without keywords. For example, if you previously issued the **ntp logging** command and you now want to disable not only the message logging, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

Examples

The following example shows how to enable NTP message logging and verify that it is enabled:

```
Router# configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# ntp logging
Router(config)# end

Router# show running-config | include ntp
ntp logging
ntp clock-period 17180152
ntp peer 10.0.0.1
ntp server 192.168.166.3
```

The following example shows how to disable NTP message logging and verify to that it is disabled:

```
Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# no ntp logging
Router# end
Router(config)# show running-config | include ntp

ntp clock-period 17180152
ntp peer 10.0.0.1
ntp server 192.168.166.3
```

The following example shows how to remove all the configured NTP options and disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
ntp peer	Configures the software clock to synchronize a peer or to be synchronized by a peer.
ntp server	Allows the software clock to be synchronized by an NTP time server.

ntp master

To configure the Cisco IOS software as a Network Time Protocol (NTP) master clock to which peers synchronize themselves when an external NTP source is not available, use the **ntp master** command in global configuration mode. To disable the master clock function, use the **no** form of this command.

ntp master [*stratum*]

no ntp [**master**]

Caution Use this command with caution. Valid time sources can be easily overridden using this command, especially if a low stratum number is configured. Configuring multiple devices in the same network with the **ntp master** command can cause instability in keeping time if the devices do not agree on the time.

Syntax Description

stratum	(Optional) Number from 1 to 15. Indicates the NTP stratum number that the system will claim.

Command Default

By default, the master clock function is disabled. When enabled, the default stratum is 8.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was modified. Support for IPv6 was added.
12.2(33)SXJ	This command was modified. Support for IPv6 was added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

Because the Cisco implementation of NTP does not support directly attached radio or atomic clocks, the router is normally synchronized, directly or indirectly, to an external system that has such a clock. In a network without Internet connectivity, such a time source may not be available. The **ntp master** command is used in such cases.

A system with the **ntp master** command configured that cannot reach any clock with a lower stratum number will claim to be synchronized at the configured stratum number, and other systems will be willing to synchronize to it via NTP.

Note The software clock must have been set from some source, including manual setting, before the **ntp master** command will have any effect. This protects against distributing erroneous time after the system is restarted.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp master** command, the NTP service is activated (if it has not already been activated) and the Cisco IOS software is configured as an NTP master clock simultaneously. When you enter the **no ntp master** command, only the NTP master clock configuration is removed from the NTP service. The NTP service itself remains active, along with any other functions that you previously configured.

To disable the NTP service on a device, you must enter the **no ntp** command without any keywords in global configuration mode. For example, if you had previously issued the **ntp master** command and you now want to remove not only the master clock function, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

Examples

The following example shows how to configure a router as an NTP master clock to which peers may synchronize:

```
Router(config)# ntp master 10
```

The following example shows how to remove all the configured NTP options and disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
clock calendar-valid	Configures the system hardware clock that is an authoritative time source for the network.

ntp max-associations

To configure the maximum number of Network Time Protocol (NTP) peers and clients for a routing device, use the **ntp max-associations** command in global configuration mode. To return the maximum associations value to the default, use the **no** form of this command.

ntp max-associations *number*

no ntp [**max-associations**]

Syntax Description

number	Number of NTP associations. The range is from 1 to 4294967295. The default is 100. In the Cisco IOS Release 12.2SX train, the range is from 0 to 4294967295.

Command Default

The maximum association value of NTP peers and clients is 100.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was modified. Support for IPv6 was added.
12.2(33)SXJ	This command was modified. Support for IPv6 was added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

The router can be configured to define the maximum number of NTP peer and client associations that the router will serve. Use the **ntp max-associations** command to set the maximum number of NTP peer and client associations that the router will serve.

The **ntp max-associations** command is useful for ensuring that the router is not overwhelmed by NTP synchronization requests. For an NTP master server, this command is useful for allowing numerous devices to synchronize to a router.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp max-associations** command, the NTP service is activated (if it has not already been activated) and the maximum number of NTP peers and clients is configured simultaneously.

In the **no** form of any **ntp** command, all the keywords are optional. When you enter the **no ntp max-associations** command, only the maximum number value is removed from the NTP service. The NTP service itself remains active, along with any other functions that you previously configured.

To disable the NTP service on a device, you must enter the **no ntp** command without any keywords in global configuration mode. For example, if you previously issued the **ntp max-associations** command and you now want to remove not only that maximum value, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

Note By default, the previous configuration values are retained when the last valid configuration (configuration for which the NTP service needs to run) is removed. Only the configuration values related to the maximum number of NTP peer and client associations are reset to the default value when the NTP process is disabled.

Examples

In the following example, the router is configured to act as an NTP server to 200 clients:

```
Router(config)# ntp max-associations 200
```

The following example shows how to remove all the configured NTP options and disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
show ntp associations	Displays all current NTP associations for the device.

ntp multicast

To configure a system to send Network Time Protocol (NTP) multicast packets on a specified interface, use the **ntp multicast** command in interface configuration mode. To disable this capability, use the **no** form of this command.

ntp multicast [*ip-address* | *ipv6-address*] [**key** *key-id*] [**ttl** *value*] [**version** *number*]

no ntp [**multicast** [*ip-address* | *ipv6-address*] [**key** *key-id*] [**ttl** *value*] [**version** *number*]]

Syntax Description

ip-address	(Optional) IPv4 address of the multicast group. Default address is 224.0.1.1.
ipv6-address	(Optional) IPv6 address of the multicast group. The address can be the all-nodes IPv6 address (FF02::1) or any other IPv6 multicast address.
key	(Optional) Defines a multicast authentication key.
key-id	(Optional) Authentication key number in the range from 1 to 4294967295. In the Cisco IOS Release 12.2SX train, the range is from 0 to 4294967295.
ttl	(Optional) Defines the time-to-live (TTL) value of a multicast NTP packet.
value	(Optional) TTL value in the range from 1 to 255. Default TTL value is 16.
version	(Optional) Defines the NTP version number.
number	(Optional) NTP version number in the range from 2 to 4. Default version number for IPv4 is 3, and default number for IPv6 is 4. In the Cisco IOS Release 12.2SX train, the range is from 1 to 4.

Command Default

NTP multicast capability is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was modified. Support for NTPv4 and IPv6 was added. The *ipv6-address* argument was added.
12.2(33)SXJ	This command was modified. Support for NTPv4 and IPv6 was added. The *ipv6-address* argument was added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

The TTL value is used to limit the scope of an audience for multicast routing.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp multicast** command, the NTP service is activated (if it has not already been activated) and the interface on which to send multicast packets is configured simultaneously.

In the **no** form of any **ntp** command, all the keywords are optional. When you enter the **no ntp multicast** command, only the multicast capability is removed from the NTP service. The NTP service itself remains active, along with any other functions that you previously configured.

To disable the NTP service on a device, you must enter the **no ntp** command in global configuration mode without keywords. For example, if you had previously issued the **ntp multicast** command and you now want to remove not only the multicast capability, but also all NTP functions from the device, use the **no ntp** command in global configuration mode without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

Examples

The following example shows how to configure Ethernet interface 0 to send NTP version 2 broadcasts:

```
Router(config)# interface ethernet 0
Router(config-if)# ntp multicast version 2
```

If you had previously issued the **ntp multicast** command and you now want to remove not only the multicast capability, but also all NTP functions from the device, use the **no ntp** command in global configuration mode without any keywords. The following example shows how to remove the **ntp multicast** command along with all the other configured NTP options and to disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
ntp authentication-key	Defines an authentication key for NTP.
ntp multicast client	Allows the system to receive NTP multicast packets on an interface.

ntp multicast client

To configure the system to receive Network Time Protocol (NTP) multicast packets on a specified interface, use the **ntp multicast client** command in interface configuration mode. To disable this capability, use the **no** form of this command.

ntp multicast client [*ip-address* | *ipv6-address*] [**novolley**]

no ntp [**multicast client** [*ip-address* | *ipv6-address*]]

Syntax Description

ip-address	(Optional) IPv4 address of the multicast group. Default address is 224.0.1.1.
ipv6-address	(Optional) IPv6 address of the multicast group. The address can be the all-nodes IPv6 address (FF02::1) or any other IPv6 multicast address.
novolley	(Optional) Disables any messages sent to the broadcast server. Avoids propagation delay by using the value configured by the **ntp broadcastdelay** command.

Command Default

NTP multicast client capability is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was modified. Support for IPv6 was added. The *ipv6-address* argument and **novolley** keyword were added.
12.2(33)SXJ	This command was modified. Support for IPv6 was added. The *ipv6-address* argument and **novolley** keyword were added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

Use the **ntp multicast client** command to allow the system to listen to multicast packets on an interface-by-interface basis.

This command enables the multicast client mode on the local NTP host. In this mode, the host is ready to receive mode 5 (broadcast) NTP messages sent to the specified multicast address. After receiving the first packet, the client measures the nominal propagation delay using a brief client/server association with the server. After this initial phase, the client enters the broadcast client mode, in which it synchronizes its clock to the received multicast messages.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp multicast client** command, the NTP service is activated (if it has not already been activated) and the interface on which to receive multicast packets is configured simultaneously.

In the **no** form of any **ntp** command, all the keywords are optional. When you enter the **no ntp multicast client** command, only the multicast client capability is removed from the NTP service. The NTP service itself remains active, along with any other functions that you previously configured.

To disable the NTP service on a device, you must enter the **no ntp** command without any keywords in global configuration mode. For example, if you had previously issued the **ntp multicast client** command and you now want to remove not only the multicast client capability, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

In IPv6 configuration, the **ntp broadcastdelay** command is used when the **ntp broadcast client** or **ntp multicast client** command is configured with the **novolley** keyword.

Examples

In the following example, the system is configured to receive (listen to) NTP multicast packets on Ethernet interface 1:

```
Router(config)# interface ethernet 1
Router(config-if)# ntp multicast client
```

If you had previously issued the **ntp multicast client** command and you now want to remove not only the multicast client capability, but also all NTP functions from the device, use the **no ntp** command without any keywords. The following example shows how to remove the **ntp multicast client** command along with all the other configured NTP options and to disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
ntp broadcast client	Configures the specified interface to receive NTP broadcast packets.
ntp broadcastdelay	Sets the estimated round-trip delay between the Cisco IOS software and an NTP broadcast server.

ntp peer

To configure the software clock to synchronize an NTP peer or to be synchronized by an NTP peer, use the **ntp peer** command in global configuration mode. To disable this capability, use the **no** form of this command.

ntp peer [**vrf** *vrf-name*] {*ip-address* | *ipv6-address* | [**ip** | **ipv6**] *hostname*} [**normal-sync**] [**version** *number*] [**key** *key-id*] [**source** *interface-type interface-number*] [**prefer**] [**maxpoll** *number*] [**minpoll** *number*] [**burst**] [**iburst**]

no ntp [**vrf** *vrf-name*] {*ip-address* | *ipv6-address* | [**ip** | **ipv6**] *hostname*}

Syntax Description

vrf *vrf-name*	(Optional) Specifies that the peer should use a named VPN routing and forwarding (VRF) instance for routing to the destination instead of to the global routing table.
ip-address	IPv4 address of the peer providing or being provided the clock synchronization.
ipv6-address	IPv6 address of the peer providing or being provided the clock synchronization.
ip	(Optional) Forces Domain Name System (DNS) resolution to be performed in the IPv4 address space.
ipv6	(Optional) Forces DNS resolution to be performed in the IPv6 address space.
hostname	Hostname of the peer that is providing or being provided the clock synchronization.
normal-sync	(Optional) Disables the rapid synchronization at startup.
version	(Optional) Defines the Network Time Protocol (NTP) version number.
number	(Optional) NTP version number (2 to 4). In the Cisco IOS Release 12.2(33)SX train, the range is from 1 to 4.
key	(Optional) Defines the authentication key.
key-id	(Optional) Authentication key to use when sending packets to this peer.
source	(Optional) Specifies that the source address must be taken from the specified interface.
interface-type	(Optional) Name of the interface from which to pick the IPv4 or IPv6 source address. For more information, use the question mark (?) online help function.
interface-number	(Optional) Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
prefer	(Optional) Makes this peer the preferred peer that provides synchronization.
maxpoll *number*	(Optional) Configures the maximum timing intervals, in seconds, between client requests sent to the server. The *number* argument ranges from 4 to 17, with 10 as the default.
minpoll *number*	(Optional) Configures the minimum timing intervals, in seconds, between client requests sent to the server. The *number* argument ranges from 4 to 17, with 6 as the default.

burst	(Optional) Enables burst mode. Burst mode allows the exchange of eight NTP messages (instead of two) during each poll interval in order to reduce the effects of network jitter.
iburst	(Optional) Enables initial burst (iburst) mode. Iburst mode triggers the immediate exchange of eight NTP messages (instead of two) when an association is first initialized. This feature allows rapid time setting at system startup or when an association is configured.

Command Default

No peers are configured.
The default **maxpoll** *number* is 10 seconds.
The default **minpoll** *number* is 6 seconds.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.3(14)T	This command was modified. The **normal-sync** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was modified. Support for IPv6 and NTPv4 was added. The **ip**, **ipv6**, **maxpoll**, **minpoll**, **burst**, and **iburst** keywords and the *ipv6-address* and *number* arguments were added.
12.2(33)SXJ	This command was modified. Support for IPv6 and NTPv4 was added. The **ip**, **ipv6**, **maxpoll**, **minpoll**, **burst**, and **iburst** keywords and the *ipv6-address* and *number* arguments were added. The command behavior was modified to display a message after selection of an unsupported NTP version.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

When a peer is configured, the default NTP version number is 3, no authentication key is used, and the source address is taken from the outgoing interface.

Use this command to allow a device to synchronize with a peer, or vice versa. Use the **prefer** keyword to reduce switching between peers.

If you are using the default version of 3 and NTP synchronization does not occur, try using NTP version 2 (NTPv2). For IPv6, use NTP version 4.

If you select an NTP version that is not supported, a message is displayed.

If you are using NTPv4, the NTP synchronization takes more time to complete (unlike NTPv3, which synchronizes in seconds or a maximum of 1 to 2 minutes). The acceptable time for synchronization in NTPv4 is 15 to 20 minutes. To achieve faster NTP synchronization, enable the burst or iburst mode by using the **burst** or **iburst** keyword. With the burst or iburst mode configured, NTP synchronization takes about 1 to 2 minutes.

The exact time span required for the NTP synchronization while using NTPv4 cannot be derived accurately. It depends on the network topology and complexity.

Multiple configurations are not allowed for the same peer or server. If a configuration exists for a peer and you use the **ntp peer** command to configure the same peer, the new configuration will replace the old one.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp peer** command, the NTP service is activated (if it has not already been activated) and the peer is configured simultaneously.

When you enter the **no ntp peer** command, only the NTP peer configuration is removed from the NTP service. The NTP service itself remains active, along with any other previously configured NTP functions.

To disable the NTP service on a device, use the **no ntp** command without keywords in global configuration mode. For example, if you had previously issued the **ntp peer** command and you now want to remove not only this restriction, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

Examples

The following example shows how to configure a router to allow its software clock to be synchronized with the clock of the peer (or vice versa) at the IPv4 address 192.168.22.33 using NTPv2. The source IPv4 address is the address of Ethernet 0:

```
Router(config)# ntp peer 192.168.22.33 version 2 source ethernet 0
```

The following example shows how to configure a router to allow its software clock to be synchronized with the clock of the peer (or vice versa) at IPv6 address 2001:0DB8:0:0:8:800:200C:417A using NTPv4:

```
Router(config)# ntp peer 2001:0DB8:0:0:8:800:200C:417A version 4
```

The following example shows how to disable rapid synchronization at startup:

```
Router(config)# ntp peer 192.168.22.33 normal-sync
```

The following example shows the message displayed when you try to configure an unsupported NTP version:

```
Router(config)# ntp peer 192.168.22.33 version 1

NTP version 4 supports backward compatibility to only version 2 and 3
 Please re-enter version[2-4]
 Setting NTP version 4 as default
```

The following example shows how to remove all the configured NTP options and disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
ntp authentication-key	Defines an authentication key for NTP.
ntp server	Allows the software clock to be synchronized by a time server.
ntp source	Uses a particular source address in NTP packets.

ntp refclock

To configure an external clock source for use with Network Time Protocol (NTP) services, use the **ntp refclock** command in line configuration mode. To disable support of the external time source, use the **no** form of this command.

ntp refclock {**trimble** | **telecom-solutions**} **pps** {**cts** | **ri** | **none**} [**inverted**] [**pps-offset** *milliseconds*] [**stratum** *number*] [**timestamp-offset** *number*]

no ntp [**refclock**]

Syntax Description

trimble	Enables the reference clock driver for the Trimble Palisade NTP Synchronization Kit (Cisco 7200 series routers only).
telecom-solutions	Enables the reference clock driver for a Telecom Solutions Global Positioning System (GPS) device.
pps	Enables a pulse per second (PPS) signal line. Indicates PPS pulse reference clock support. The options are **cts**, **ri**, or **none**.
cts	Enables PPS on the Clear To Send (CTS) line.
ri	Enables PPS on the Ring Indicator (RI) line.
none	Specifies that no PPS signal is available.
inverted	(Optional) Specifies that the PPS signal is inverted.
pps-offset *milliseconds*	(Optional) Specifies the offset of the PPS pulse. The number is the offset (in milliseconds).
stratum *number*	(Optional) Indicates the NTP stratum number that the system will claim. Number is from 0 to 14.
timestamp-offset *number*	(Optional) Specifies the offset of time stamp. The number is the offset (in milliseconds).

Command Default

By default, an external clock source for use with NTP services is not configured.

Command Modes

Line configuration (config-line)

Command History

Release	Modification
12.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was modified. Support for IPv6 was added.
12.2(33)SXJ	This command was modified. Support for IPv6 was added.

Release	Modification
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

To configure a PPS signal as the source for NTP synchronization, use the following form of the **ntp refclock** command:

ntp refclock trimble pps {**cts** | **ri**} [**inverted**] [**pps-offset** *milliseconds*] [**stratum** *number*] [**timestamp-offset** *number*]

To configure a Trimble Palisade NTP Synchronization Kit as the GPS clock source connected to the auxiliary port of a Cisco 7200 router, use the following form of the **ntp refclock** command:

ntp refclock trimble pps none [**stratum** *number*]

To configure a Telecom Solutions product as the GPS clock source, use the **ntp refclock telecom-solutions** form of the command:

ntp refclock telecom-solutions pps cts [**stratum** *number*]

When two or more servers are configured with the same stratum number, the client will never synchronize with any of the servers. This is because the client is not able to identify the device with which to synchronize. When two or more servers are configured with the same stratum number, and if the client was in synchronization with one of the servers, the synchronization is lost if the settings on one server are changed.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp refclock** command, the NTP service is activated (if it has not already been activated) and the external clock source is configured simultaneously.

In the **no** form of any **ntp** command, all the keywords are optional. When you enter the **no ntp refclock** command, only the external clock source is removed from the NTP service. The NTP service itself remains active, along with any other functions that you previously configured.

To terminate the NTP service on a device, you must enter the **no ntp** command without keywords in global configuration mode. For example, if you had previously issued the **ntp refclock** command and you now want to remove not only the external clock source, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also terminated.

Examples

The following example shows the configuration of a Trimble Palisade GPS time source on a Cisco 7200 router:

```
Router(config)# ntp master
Router(config)# ntp update-calendar
Router(config)# line aux 0
Router(config-line)# ntp refclock trimble pps none
```

The following example shows the configuration of a Telecom Solutions GPS time source on a Catalyst switch platform:

```
Router(config)# ntp master
Router(config)# ntp update-calendar
Router(config)# line aux 0
Router(config-line)# ntp refclock telecom-solutions pps cts stratum 1
```

If you had previously issued the **ntp refclock** command and you now want to remove not only the external clock source, but also all NTP functions from the device, use the **no ntp** command without any keywords in global configuration mode. The following example shows how to remove the **ntp refclock** command along with all the configured NTP options and how to disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
show ntp associations	Displays the status of NTP associations configured for your system.

ntp server

To allow the software clock to be synchronized by a Network Time Protocol (NTP) time server, use the **ntp server** command in global configuration mode. To disable this capability, use the **no** form of this command.

ntp server [**vrf** *vrf-name*] {*ip-address* | *ipv6-address* | [**ip** | **ipv6**] *hostname*} [**normal-sync**] [**version** *number*] [**key** *key-id*] [**source** *interface-type interface-number*] [**prefer**] [**maxpoll** *number*] [**minpoll** *number*] [**burst**] [**iburst**]

no ntp server [**vrf** *vrf-name*] {*ip-address* | *ipv6-address* | [**ip** | **ipv6**] *hostname*}

Syntax Description

vrf *vrf-name*	(Optional) Specifies that the peer should use a named VPN routing forwarding (VRF) instance for routing to the destination instead of to the global routing table.
ip-address	IPv4 address of the peer providing or being provided the clock synchronization.
ipv6-address	IPv6 address of the peer providing or being provided the clock synchronization.
ip	(Optional) Forces domain name server (DNS) resolution to be performed in the IPv4 address space.
ipv6	(Optional) Forces DNS resolution to be performed in the IPv6 address space.
hostname	Hostname of the peer providing or being provided the clock synchronization.
normal-sync	(Optional) Disables the rapid synchronization at startup.
version	(Optional) Defines the NTP version number.
number	(Optional) NTP version number (2 to 4). In the Cisco IOS Release 12.2SX train, the range is from 1 to 4.
key	(Optional) Defines the authentication key.
key-id	(Optional) Authentication key to use when sending packets to this peer.
source	(Optional) Specifies that the source address must be taken from the specified interface.
interface-type	(Optional) Name of the interface from which to pick the IPv4 or IPv6 source address. For more information, use the question mark (?) online help function.
interface-number	(Optional) Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
prefer	(Optional) Makes this peer the preferred peer that provides synchronization.
maxpoll *number*	(Optional) Configures the maximum timing intervals, in seconds, between client requests sent to the server. The *number* argument ranges from 4 to 17, with 10 as the default.
minpoll *number*	(Optional) Configures the minimum timing intervals, in seconds, between client requests sent to the server. The *number* argument ranges from 4 to 17, with 6 as the default.

burst	(Optional) Enables burst mode. Burst mode allows the exchange of eight NTP messages (instead of two) during each poll interval in order to reduce the effects of network jitter.
iburst	(Optional) Enables initial burst (iburst) mode. Iburst mode triggers the immediate exchange of eight NTP messages (instead of two) when an association is first initialized. This feature allows rapid time setting at system startup or when an association is configured.

Command Default

No servers are configured by default. If a server is configured, the default NTP version number is 3, an authentication key is not used, and the source IPv4 or IPv6 address is taken from the outgoing interface.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was modified. Support for IPv6 was added to NTP version 4. The **ip**, **ipv6**, **maxpoll**, **minpoll**, **burst**, and **iburst** keywords and the *number* and *ipv6-address* arguments were added.
12.2(33)SXJ	This command was modified. Support for IPv6 was added to NTP version 4. The **ip**, **ipv6**, **maxpoll**, **minpoll**, **burst**, and **iburst** keywords and the *number* and *ipv6-address* arguments were added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

Use this command if you want to allow the system to synchronize with the specified server.

When you use the *hostname* option, the router does a DNS lookup on that name, and stores the IPv4 or IPv6 address in the configuration. For example, if you enter the **ntp server** *hostname* command and then check the running configuration, the output shows "ntp server *a.b.c.d*," where *a.b.c.d* is the IP address of the host, assuming that the router is correctly configured as a DNS client.

Use the **prefer** keyword if you need to use this command multiple times, and you want to set a preferred server. Using the **prefer** keyword reduces switching between servers.

If you are using the default NTP version 3 and NTP synchronization does not occur, try NTPv2. Some NTP servers on the Internet run version 2. For IPv6, use NTP version 4.

If you are using NTPv4, the NTP synchronization takes more time to complete (unlike NTPv3, which synchronizes in seconds or a maximum of 1 to 2 minutes). The acceptable time for synchronization in NTPv4 is 15 to 20 minutes. To achieve faster NTP synchronization, enable the burst or iburst mode by using the **burst** or **iburst** keyword. With the burst or iburst mode configured, NTP synchronization takes about 1 to 2 minutes.

The exact time span required for the NTP synchronization while using NTPv4 cannot be derived accurately. It depends on the network topology and complexity.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp server** command, the NTP service is activated (if it has not already been activated) and software clock synchronization is configured simultaneously.

When you enter the **no ntp server** command, only the server synchronization capability is removed from the NTP service. The NTP service itself remains active, along with any other previously configured NTP functions.

To disable the NTP service on a device, enter the **no ntp** command without keywords. For example, if you had previously issued the **ntp server** command and you now want to remove not only the server synchronization capability, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

If you want to unconfigure an NTP server or a peer configured with a particular source interface, you must specify the interface type and number in the **no** form of the command.

Examples

The following example shows how to configure a router to allow its software clock to be synchronized with the clock by using the device at the IPv4 address 172.16.22.44 using NTPv2:

```
Router(config)# ntp server 172.16.22.44 version 2
```

The following example shows how to configure a router to allow its software clock to be synchronized with the clock by using the device at the IPv6 address 2001:0DB8:0:0:8:800:200C:417A using NTPv4:

```
Router(config)# ntp server 2001:0DB8:0:0:8:800:200C:417A version 4
```

The following example shows how to configure an NTP peer with a particular source interface:

```
Router(config)# ntp server 209.165.200.231 source ethernet 0/1
```

Related Commands

Command	Description
ntp authentication-key	Defines an authentication key for NTP.
ntp peer	Configures the software clock to synchronize a peer or to be synchronized by a peer.
ntp source	Uses a particular source address in NTP packets.

ntp source

To use a particular source address in Network Time Protocol (NTP) packets, use the **ntp source** command in global configuration mode. To remove the specified source address, use the **no** form of this command.

ntp source *interface-type interface-number*

no ntp [**source**]

Syntax Description

interface-type	Type of interface.
interface-number	Number of the interface.

Command Default

Source address is determined by the outgoing interface.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was modified. Support was added to allow a specified interface to be configured with IPv6 addresses.
12.2(33)SXJ	This command was modified. Support was added to allow a specified interface to be configured with IPv6 addresses.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

Use this command when you want to use a particular source IPv4 or IPv6 address for all NTP packets. The address is taken from the named interface. This command is useful if the address on an interface cannot be used as the destination for reply packets. If the **source** keyword is present on an **ntp server** or **ntp peer** global configuration command, that value overrides the global value set by this command.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp source** command, the NTP service is activated (if it has not already been activated) and the source address is configured simultaneously.

In the **no** form of any **ntp** command, all the keywords are optional. When you enter the **no ntp source** command, only the source address is removed from the NTP service. The NTP service itself remains active, along with any other functions that you previously configured.

To disable the NTP service on a device, you must enter the **no ntp** command without any keywords in global configuration mode. For example, if you had previously issued the **ntp source** command and you now want to remove not only the configured source address, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

If the NTP source is not set explicitly, and a link fails or an interface state changes, the NTP packets are sourced from the next best interface and the momentarily lost synchronization is regained.

Examples

The following example shows how to configure a router to use the IPv4 or IPv6 address of Ethernet interface 0 as the source address of all outgoing NTP packets:

```
Router(config)# ntp source ethernet 0
```

The following example shows how to remove all the configured NTP options and disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
ntp peer	Configures the software clock to synchronize a peer or to be synchronized by a peer.
ntp server	Allows the software clock to be synchronized by a time server.

ntp trusted-key

To authenticate the identity of a system to which Network Time Protocol (NTP) will synchronize, use the **ntp trusted-key** command in global configuration mode. To disable the authentication of the identity of the system, use the **no** form of this command.

ntp trusted-key *key-number*

no ntp [**trusted-key** *key-number*]

Syntax Description

key-number	Key number of the authentication key to be trusted.

Command Default

Authentication of the identity of the system is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was modified. Support for IPv6 was added.
12.2(33)SXJ	This command was modified. Support for IPv6 was added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

If authentication is enabled, use this command to define one or more key numbers (corresponding to the keys defined with the **ntp authentication-key** command) that a peer NTP system must provide in its NTP packets for synchronization. This function provides protection against accidentally synchronizing the system to a system that is not trusted, because the other system must know the correct authentication key.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp trusted-key** command, the NTP service is activated (if it has not already been activated) and the system to which NTP will synchronize is authenticated simultaneously.

In the **no** form of any **ntp** command, all the keywords are optional. When you enter the **no ntp trusted-key** command, only the authentication is disabled in the NTP service. The NTP service itself remains active, along with any other functions that you previously configured.

To disable the NTP service on a device, you must enter the **no ntp** command without any keywords in global configuration mode. For example, if you had previously issued the **ntp trusted-key** command and you now want to remove not only the authentication, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

Examples

The following example shows how to configure the system to synchronize only to systems providing authentication key 42 in its NTP packets:

```
Router(config)# ntp authenticate
Router(config)# ntp authentication-key 42 md5 aNiceKey
Router(config)# ntp trusted-key 42
```

The following example shows how to remove all the configured NTP options and disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
ntp authenticate	Enables NTP authentication.
ntp authentication-key	Defines an authentication key for NTP.

ntp update-calendar

To periodically update the hardware clock (calendar) from a Network Time Protocol (NTP) time source, use the **ntp update-calendar** command in global configuration mode. To disable the periodic updates, use the **no** form of this command.

ntp update-calendar

no ntp [**update-calendar**]

Syntax Description

This command has no arguments or keywords.

Command Default

The hardware clock (calendar) is not updated.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was modified. Support for IPv6 was added.
12.2(33)SXJ	This command was modified. Support for IPv6 was added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

Some platforms have a battery-powered hardware clock, referred to in the CLI as the calendar, in addition to the software-based system clock. The hardware clock runs continuously, even if the router is powered off or rebooted.

If the software clock is synchronized to an outside time source via NTP, it is a good practice to periodically update the hardware clock with the time learned from NTP. Otherwise, the hardware clock will tend to gradually lose or gain time (drift), and the software clock and hardware clock may lose synchronization with each other. The **ntp update-calendar** command will enable the hardware clock to be periodically updated with the time specified by the NTP source. The hardware clock will be updated only if NTP has synchronized to an authoritative time server.

Many lower-end routers (for example, the Cisco 2500 series or the Cisco 2600 series) do not have hardware clocks, so this command is not available on those platforms.

To force a single update of the hardware clock from the software clock, use the **clock update-calendar** command in user EXEC mode.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp update-calendar** command, the NTP service is activated (if it has not already been activated) and the hardware clock is updated simultaneously.

In the **no** form of any **ntp** command, all the keywords are optional. When you enter the **no ntp update-calendar** command, only the clock updates are stopped in the NTP service. The NTP service itself remains active, along with any other functions that you previously configured.

To disable the NTP service on a device, you must enter the **no ntp** command without any keywords in global configuration mode. For example, if you had previously issued the **ntp update-calendar** command and you now want to disable not only the periodic updates, but also all NTP functions running on the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

Examples

The following example shows how to configure the system to periodically update the hardware clock from the NTP time source:

```
Router(config)# ntp update-calendar
```

The following example shows how to remove all the configured NTP options and disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
clock read-calendar	Performs a one-time update of the software clock from the hardware clock (calendar).
clock update-calendar	Performs a one-time update of the hardware clock (calendar) from the software clock.

ospfv3 area

To enable Open Shortest Path First version 3 (OSPFv3) on an interface with the IPv4 or IPv6 address family (AF), use the **ospfv3 area** command in interface configuration mode. To disable OSPFv3 routing for interfaces defined, use the **no** form of this command.

ospfv3 *process-id* **area** *area-ID* {**ipv4** | **ipv6**} [**instance** *instance-id*]

no ospfv3 *process-id* **area** *area-ID* {**ipv4** | **ipv6**}

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
area-id	Area that is to be associated with the OSPFv3 interface.
ipv4	IPv4 address family.
ipv6	IPv6 address family.
instance *instance-id*	(Optional) Instance identifier. • When the **ipv4** keyword is used, the *instance-id* argument can be a value from 64 through 95. The default is 64. • When the **ipv6** keyword is used, the *instance-id* argument can be a value from 0 through 31. The default is 0.

Command Default

OSPFv3 is not enabled on the interface.
The default instance ID for IPv4 is 64.
The default instance ID for IPv6 is 0.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

Use the **ospfv3 area** command to enable OSPFv3 on an interface. This command enables you to configure two OSPFv3 instances on an interface–one IPv6 AF instance, and one IPv4 AF instance. You can configure only one process for each AF per interface.

Before you enable OSPFv3 on an interface using the **ospfv3 area** command, you must enable IPv6 on the interface, and you must enable IPv6 routing.

When the **ospfv3 area** command is configured for the IPv6 AF, it overwrites the **ipv6 ospf area** configuration if OSPFv3 was attached to the interface using the **ipv6 ospf area** command.

Examples

The following example enables OSPFv3 for the IPv4 AF on an interface:

```
Router(config)# interface ethernet0/0
Router(config-if)# ospfv3 1 area 1 ipv4
```

ospfv3 authentication

To specify the authentication type for an Open Shortest Path First version 3 (OSPFv3) instance, use the **ospfv3 authentication** command in interface configuration mode. To remove this instance, use the **no** form of this command.

ospfv3 authentication {**ipsec** *spi*} {**md5** | **sha1**} {*key-encryption-type key*} | **null**

no ospfv3 authentication {**ipsec** *spi*} {**md5** | **sha1**} {*key-encryption-type key*} | **null**

Syntax Description

ipsec	Configures use of IP Security (IPsec) authentication.
spi *spi*	Security policy index (SPI) value. The *spi* value must be a number from 256 to 4294967295.
md5	Enables message digest 5 (MD5) authentication.
sha1	Enables Secure Hash Algorithm 1 (SHA-1) authentication.
key-encryption-type	One of the following values can be entered: • **0**—The key is not encrypted. • **7**—The key is encrypted.
key	Number used in the calculation of the message digest. • When MD5 authentication is used, the key must be 32 hex digits (16 bytes) long. • When SHA-1 authentication is used, the key must be 40 hex digits (20 bytes) long.
null	Used to override area authentication.

Command Default

No authentication is specified.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

Use the **ospfv3 authentication** command to specify the OSPFv3 authentication type on an interface. The **ospfv3 authentication** command cannot be configured per process. If the **ospfv3 authentication** command is used, it affects all OSPFv3 instances.

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

The policy database is common to all client applications on a box. This means that two IPsec clients, such as OSPFv3 and a tunnel, cannot use the same SPI. Additionally, an SPI can be used only in one policy.

The **null** keyword is used to override existing area authentication. If area authentication is not configured, then it is not necessary to configure the interface with the **authentication null** command.

Examples

The following example specifies the authentication type for an OSPFv3 instance: :

```
Router(config)# interface ethernet0/0
Router(config-if)# ospfv3 authentication md5 0 275761340947681324733020312097 27
```

Related Commands

Command	Description
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

ospfv3 cost

To explicitly specify the cost of sending a packet on an Open Shortest Path First version 3 (OSPFv3) interface, use the **ospfv3 cost** command in interface configuration mode. To reset the interface cost to the default value, use the **no** form of this command.

ospfv3 [*process-id*] **cost** {*interface-cost* | **dynamic** [**default** *default-link-metric* | **hysteresis** [*percent* | **threshold** *threshold-value*] | **weight** {**L2-factor** *percent* | **latency** *percent* | **resources** *percent* | **throughput** *percent*}

no ospfv3 [*process-id*] **cost**

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
interface-cost	Route cost of this interface. It can be a value in the range from 1 to 65535.
dynamic	Default value on VMI interfaces.
default	(Optional) Default link metric value.
default-link-metric	Specifies the default link metric value on this interface. It can be a value in the range from 0 to 65535.
hysteresis	(Optional) Hysteresis value for link-state advertisement (LSA) dampening.
percent	(Optional) The percentage of c
threshold *threshold-value*	(Optional) Cost change threshold at which hysteresis will be implemented. The threshold range is from 0 to 64k, and the default threshold value is 10k.
weight	(Optional) Amount of impact a variable has on the dynamic cost.
L2-factor *percent*	Quality weight of the Layer 2 link expressed as a percentage. The *percent* value can be in the range from 0 to 100. The default value is 100.
latency *percent*	Latency weight of the Layer 2 link, expressed as a percentage. The *percent* value can be in the range from 0 to 100. The default value is 100.
resources *percent*	Resources weight (such as battery life) of the router at the Layer 2 link, expressed as a percentage. The *percent* value can be in the range from 0 to 100. The default value is 100.
throughput *percent*	Throughput weight of the Layer 2 link, expressed as a percentage. The *percent* value can be in the range from 0 to 100. The default value is 100.

Command Default

Default cost is based on the bandwidth. Mobile Ad Hoc Network (MANET) interfaces are set to use dynamic costs. Non-MANET networks are set to use static costs.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

Use the **ospfv3 cost** command to specify the cost of sending a packet on an interface. When the **ospfv3 cost** command is configured with the *process-id* argument, it overwrites the **ipv6 ospf cost** configuration if OSPFv3 was attached to the interface using the **ipv6 ospf area** command. When the **ospfv3 cost** command is configured without the *process-id* argument, it is inherited on all instances running on the interface.

You can set the metric manually using the **ospfv3 cost** command, if you need to change the default. Using the **bandwidth** command changes the link cost as long as the **ospfv3 cost** command is not used. The link-state metric is advertised as the link cost in the router link advertisement.

The dynamic cost metric used for interfaces is computed based on the Layer 2 (L2) feedback to Layer 3 (L3). For a dynamic cost to have the same cost as a default cost, all parameters must equal zero.

Each Layer 2 feedback can contribute a cost in the range of 0 to 65535. To tune down this cost range, use the optional **weight** keyword in conjunction with the **throughput**, **resources**, **latency**, or **L2-factor** keyword. Each of these weights has a default value of 100% and can be configured in the range from 0 to 100. When 0 is configured for a specific weight, that weight does not contribute to the OSPFv3 cost.

Because cost components can change rapidly, you may need to dampen the amount of changes in order to reduce network-wide churn. Use the optional **hysteresis** keyword with the **threshold** *threshold-value* keyword and argument to set a cost change threshold. Any cost change below this threshold is ignored.

If you enable hysteresis without specifying the mode (percent or threshold), the default mode is threshold, and 10k as the default threshold value.

The higher the threshold or the percent value is set, the larger the change in link quality required to change the OSPFv3 route costs.

Mobile Ad Hoc Networks (MANET)

When the network type is set to MANET, the OSPF cost associated with an interface automatically sets to dynamic. All other network types, keep the interface cost, and you must enter the **ospfv3 cost dynamic** command to change the cost to dynamic.

If you do not specify a default dynamic cost with the **ospfv3 cost dynamic default** command, OSPF uses the interface cost until it receives link metric data.

Examples

The following example sets the interface cost value to 65:

```
Router(config)# interface ethernet0/0
Router(config-if)# ospfv3 101 cost 65
```

The following example shows how to configure OSPFv3 instance 4 to use 30 as the default cost until link metric data arrives from dynamic costing:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ospfv3 4 cost dynamic default 30
Router(config-if)# exit
```

Related Commands

Command	Description
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

ospfv3 database-filter

To filter outgoing link-state advertisements (LSAs) to an Open Shortest Path First version 3 (OSPFv3) interface, use the **database-filter** command in interface configuration mode. To restore the forwarding of LSAs to the interface, use the **no** form of this command.

ospfv3 [*process-id*] **database-filter** [**all** | **disable**]

no ospfv3 database-filter

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
all	(Optional) Filters all LSAs on the OSPFv3 interface.
disable	(Optional) Disables the LSA filter on the OSPFv3 interface.

Command Default

All outgoing LSAs are flooded to the interface.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

Use the **ospfv3 database-filter** command to filter outgoing LSAs to an OSPFv3 interface. When the **ospfv3 database-filter** command is configured with the *process-id* argument, it overwrites the **ipv6 ospf database-filter** configuration if OSPFv3 was attached to the interface using the **ipv6 ospf area** command. When the **ospfv3 database-filter** command is configured without the *process-id* argument, it is inherited on all instances running on the interface.

Examples

The following example prevents flooding of OSPFv3 LSAs to networks reachable through Ethernet interface 0/0:

```
Router(config)# interface ethernet0/0
Router(config-if)# ospfv3 101 database-filter
```

Related Commands

Command	Description
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

ospfv3 dead-interval

To set the time period for which hello packets must not be seen before neighbors declare the router down, use the **ospfv3 dead-interval** command in interface configuration mode. To return to the default time, use the **no** form of this command.

ospfv3 [*process-id*] **dead-interval** *seconds*

no ospfv3 [*process-id*] **dead-interval** *seconds*

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
seconds	Specifies the interval (in seconds). The value must be the same for all nodes on the network. The value can be from 1 through 65335 seconds.

Command Default

Four times the interval set by the **ospfv3 hello-interval** command.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

Use the **ospfv3 dead-interval** command to set the time period for which hello packets must not be seen before neighbors declare the router down. When the **ospfv3 dead-interval** command is configured with the *process-id* argument, it overwrites the **ipv6 dead-interval** configuration if OSPFv3 was attached to the interface using the **ipv6 ospf area** command. When the **ospfv3 dead-interval** command is configured without the *process-id* argument, it is inherited on all instances running on the interface.

The interval is advertised in router hello packets. This value must be the same for all routers and access servers on a specific network.

If no hello-interval is specified, the default dead-interval is 120 seconds for Mobile Ad Hoc Networks (MANETs) and 40 seconds for all other network types.

Examples

The following example sets the OSPFv3 dead interval to 60 seconds:

```
Router(config)# interface ethernet0/0
Router(config-if)# ospfv3 101 dead-interval 60
```

Related Commands

Command	Description
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

ospfv3 demand-circuit

To configure Open Shortest Path First version 3 (OSPFv3) to treat the interface as an OSPFv3 demand circuit, use the **ospfv3 demand-circuit** command in interface configuration mode. To remove the demand circuit designation from the interface, use the **no** form of this command.

ospfv3 [*process-id*] **demand-circuit** [**disable**]

no ospfv3 demand-circuit

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
disable	(Optional) Disables the demand circuit on the specified OSPFv3 instance.

Command Default

The circuit is not a demand circuit.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

Use the **ospfv3 demand-circuit** command to configure OSPFv3 to treat the interface as an OSPFv3 demand circuit. When the **ospfv3 demand-circuit** command is configured with the *process-id* argument, it overwrites the **ipv6 ospf demand-circuit** configuration if OSPFv3 was attached to the interface using the **ipv6 ospf area** command. When the **ospfv3 demand-circuit** command is configured without the *process-id* argument, it is inherited on all instances running on the interface.

On point-to-point interfaces, only one end of the demand circuit must be configured with the **demand-circuit** command. Periodic hello messages are suppressed and periodic refreshes of link-state advertisements (LSAs) do not flood the demand circuit. This command allows the underlying data link layer to be closed when the topology is stable. In point-to-multipoint topology, only the multipoint end must configured with this command.

Examples

The following example configures an on-demand circuit on Ethernet interface 0/0:

```
Router(config)# interface ethernet0/0
Router(config-if)# ospfv3 101 demand-circuit
```

Related Commands

Command	Description
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

ospfv3 encryption

To specify the encryption type for an Open Shortest Path First version 3 (OSPFv3) interface, use the **ospfv3 encryption** command in interface configuration mode. To remove the encryption type from an interface, use the **no** form of this command.

ospfv3 encryption {**ipsec spi** *spi* **esp** *encryption-algorithm* {*key-encryption-type key*} *authentication-algorithm* {*key-encryption-type key*} | **null**}

no ospfv3 encryption ipsec spi *spi*

Syntax Description

ipsec	Configures use of IP Security (IPsec) authentication.
spi *spi*	Security policy index (SPI) value. The *spi* value must be a number from 256 to 4294967295.
esp	Encapsulating security payload (ESP).
encryption-algorithm	Encryption algorithm to be used with ESP. The values can be any of the following: • **aes-cdc**—Enables AES-CDC encryption. • **3des**—Enables 3DES encryption. • **des**—Enables DES encryption. • **null**—ESP with no encryption.
key-encryption-type	One of two values can be entered: • **0**—The key is not encrypted. • **7**—The key is encrypted.
key	Number used in the calculation of the message digest. • When MD5 authentication is used, the key must be 32 hex digits (16 bytes) long. • When SHA-1 authentication is used, the key must be 40 hex digits (20 bytes) long.
authentication-algorithm	Encryption authentication algorithm to be used. The values can be one of the following: • **md5**—Enables message digest 5 (MD5). • **sha1**—Enables SHA-1.
null	Overrides area encryption.

Command Default

Authentication and encryption are not configured on an interface.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

Use the **ospfv3 encryption** command to specify the encryption type for an interface. The **ospfv3 encryption** command cannot be configured per process. If the **ospfv3 encryption** command is used, it affects all OSPFv3 instances.

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

The policy database is common to all client applications on a box. This means that two IPSec clients, such as OSPFv3 and a tunnel, cannot use the same SPI. Additionally, an SPI can be used only in one policy.

The **null** keyword is used to override existing area encryption. If area encryption is not configured, then it is not necessary to configure the interface with the **encryption null** command.

Examples

The following example specifies the encryption type for Ethernet interface 0/0. The IPSec SPI value is 1001, ESP is used with no encryption, and the authentication algorithm is MD5.

```
Router(config)# interface ethernet 0/0
Router(config-if)# ospfv3 encryption ipsec spi 1001 esp null md5 0
275761340947681324733020312097 27
```

Related Commands

Command	Description
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

ospfv3 flood-reduction

To suppress the unnecessary flooding of link-state advertisements (LSAs) in stable topologies, use the **ospfv3 flood-reduction** command in interface configuration mode. To disable this feature, use the **no** form of this command.

ospfv3 [*process-id*] **flood-reduction** [**disable**]

no ospfv3 [*process-id*] **flood-reduction**

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the Open Shortest Path First version 3 (OSPFv3) routing process and can be a value from 1 through 65535.
disable	(Optional) Allows flood reduction to be disabled on the specified OSPFv3 interface.

Command Default

This command is disabled.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

Use the **ospfv3 flood-reduction** command to suppress unnecessary LSA flooding in stable topologies. When the **ospfv3 flood-reduction** command is configured with the *process-id* argument, it overwrites the **ipv6 ospf flood-reduction** configuration if OSPFv3 was attached to the interface using the **ipv6 ospf flood-reduction** command. When the **ospfv3 flood-reduction** command is configured without the *process-id* argument, it is inherited on all instances running on the interface.

All routers supporting the OSPFv3 demand circuit are compatible and can interact with routers supporting flooding reduction.

Examples

The following example suppresses the flooding of unnecessary LSAs on Ethernet interface 0/0:

```
Router(config)# interface ethernet0/0
Router(config-if)# ospfv3 101 flood-reduction
```

Related Commands

Command	Description
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

ospfv3 hello-interval

To specify the interval between hello packets that the Cisco IOS software sends on the Open Shortest Path First version 3 (OSPFv3) interface, use the **ospfv3 hello-interval** command in interface configuration mode. To return to the default time, use the **no** form of this command.

ospfv3 [*process-id*] **hello-interval** *seconds*

no ospfv3 [*process-id*] **hello-interval** *seconds*

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
seconds	Specifies the interval (in seconds). The value must be the same for all nodes on a specific network.

Command Default

The default interval is 10 seconds when using Ethernet and 30 seconds when using nonbroadcast, such as Mobile Ad Hoc Networks (MANETs).

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

Use the **ospfv3 hello-interval** command to suppress unnecessary LSA flooding in stable topologies. When the **ospfv3 hello-interval** command is configured with the *process-id* argument, it overwrites the **ipv6 ospf hello-interval** configuration if OSPFv3 was attached to the interface using the **ipv6 ospf area** command. When the **ospfv3 hello-interval** command is configured without the *process-id* argument, it is inherited on all instances running on the interface.

The **hello-interval** value is advertised in the hello packets. The shorter the hello interval, the earlier topological changes will be detected, but more routing traffic will ensue. This value must be the same for all routers and access servers on a specific network.

Examples

The following example sets the interval between hello packets to 15 seconds:

```
Router(config)# interface ethernet0/0
Router(config-if)# ospfv3 101 hello-interval 15
```

Related Commands

Command	Description
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

ospfv3 mtu-ignore

To disable Open Shortest Path First version 3 (OSPFv3) maximum transmission unit (MTU) mismatch detection on receiving database descriptor (DBD) packets, use the **ospfv3 mtu-ignore** command in interface configuration mode. To reset to default, use the **no** form of this command.

ospfv3 [*process-id*] **mtu-ignore** [**disable**]

no ospfv3 [*process-id*] **mtu-ignore**

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
disable	(Optional) Allows **mtu-ignore** to be disabled on the specified OSPFv3 interface.

Command Default

OSPFv3 MTU mismatch detection is enabled.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

Use the **ospfv3 mtu-ignore** command to disable OSPFv3 MTU mismatch detection on receiving DBD packets. When the **ospfv3 mtu-ignore** command is configured with the *process-id* argument, it overwrites the **ipv6 ospf mtu-ignore** configuration if OSPFv3 was attached to the interface using the **ipv6 ospf area** command. When the **ospfv3 mtu-ignore** command is configured without the *process-id* argument, it is inherited on all instances running on the interface.

OSPFv3 checks whether neighbors are using the same MTU on a common interface. This check is performed when neighbors exchange DBD packets. If the receiving MTU in the DBD packet is higher then the IP MTU configured on the incoming interface, OSPFv3 adjacency will not be established.

Examples

The following example disables MTU mismatch detection on receiving DBD packets:

```
Router(config)# interface ethernet0/0
Router(config-if)# ospfv3 101 mtu-ignore
```

Related Commands

Command	Description
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

ospfv3 network

To configure an Open Shortest Path First version 3 (OSPFv3) network type to a type other than the default for a given medium, use the **ospfv3 network** command in interface configuration mode. To return to the default type, use the **no** form of this command.

ospfv3 [*process-id*] **network** {**broadcast** | **manet** | **non-broadcast** | {**point-to-multipoint** [**non-broadcast**] | **point-to-point**}}

no ospfv3 [*process-id*] **network** {**broadcast** | **manet** | **non-broadcast** | {**point-to-multipoint** [**non-broadcast**] | **point-to-point**}}

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
broadcast	Sets the network type to broadcast.
manet	Sets the network type to Mobile Ad Hoc Network (MANET).
non-broadcast	Sets the network type to nonbroadcast multiaccess (NBMA).
point-to-multipoint [**non-broadcast**]	Sets the network type to point-to-multipoint. The optional **non-broadcast** keyword sets the point-to-multipoint network to be nonbroadcast. If you use the **non-broadcast** keyword, the **neighbor** command is required.
point-to-point	Sets the network type to point-to-point.

Command Default

Default depends on the network type.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

Use the **ospfv3 network** command to configure an OSPFv3 network type to a type other than the default for a given medium. When the **ospfv3 network** command is configured with the *process-id* argument, it overwrites the **ipv6 ospf network** configuration if OSPFv3 was attached to the interface using the **ipv6 ospf area** command. When the **ospfv3 network** command is configured without the *process-id* argument, it is inherited on all instances running on the interface. .

MANET Networks

Use the **ospfv3 network manet** command to enable relaying and caching of LSA updates and LSA ACKs on the MANET interface. This results in a reduction of OSPF traffic and saves radio bandwidth.

By default, selective peering is disabled on MANET interfaces.

By default, the OSPFv3 dynamic cost timer is enabled for the MANET network type, as well as caching of LSAs and LSA ACKs received on the MANET interface. The following default values are applied for cache and timers:

LSA cache	Default = 1000 messages
LSA timer	Default = 10 minutes
LSA ACK cache	Default = 1000 messages
LSA ACK timer	Default = 5 minutes

Examples

The following example sets your OSPFv3 network as a broadcast network:

```
Router(config)# interface ethernet0/0
Router(config-if)# ospfv3 101 network broadcast
```

Related Commands

Command	Description
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

ospfv3 priority

To set the router priority, which helps determine the designated router for this network, use the **ospfv3 priority** command in interface configuration mode. To return to the default value, use the **no** form of this command.

ospfv3 [*process-id*] **priority** *number-value*

no ospfv3 [*process-id*] **priority** *number-value*

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the Open Shortest Path First version 3 (OSPFv3) routing process and can be a value from 1 through 65535.
number-value	A number value that specifies the priority of the router. The range is from 0 to 255.

Command Default

The router priority is 1.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

Use the **ospfv3 priority** command to set the router priority, which helps determine the designated router for this network. When the **ospfv3 priority** command is configured with the *process-id* argument, it overwrites the **ipv6 ospf priority** configuration if OSPFv3 was attached to the interface using the **ipv6 ospf area** command. When the **ospfv3 priority** command is configured without the *process-id* argument, it is inherited on all instances running on the interface.

When two routers attached to a network both attempt to become the designated router, the one with the higher router priority takes precedence. If there is a tie, the router with the higher router ID takes precedence. A router with a router priority set to zero is ineligible to become the designated router or backup designated router. Router priority is configured only for interfaces to multiaccess networks (in other words, not to point-to-point networks).

Examples

The following example sets the router priority value to 4:

```
Router(config)# interface ethernet0/0
Router(config-if)# ospfv3 101 priority 4
```

Related Commands

Command	Description
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

ospfv3 retransmit-interval

To specify the time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the Open Shortest Path First version 3 (OSPFv3) interface, use the **ospfv3 retransmit-interval** command in interface configuration mode. To return to the default value, use the **no** form of this command.

ospfv3 [*process-id*] **retransmit-interval** *seconds*

no ospfv3 [*process-id*] **retransmit-interval** *seconds*

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
seconds	Time (in seconds) between retransmissions. It must be greater than the expected round-trip delay between any two routers on the attached network. The range is from 1 to 65535 seconds, and the default is 5 seconds.

Command Default

The default is 5 seconds.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

Use the **ospfv3 retransmit-interval** command to specify the time between LSA retransmissions for adjacencies belonging to the interface. When the **ospfv3 retransmit-interval** command is configured with the *process-id* argument, it overwrites the **ipv6 ospf retransmit-interval** configuration if OSPFv3 was attached to the interface using the **ipv6 ospf area** command. When the **ospfv3 retransmit-interval** command is configured without the *process-id* argument, it is inherited on all instances running on the interface.

When a router sends an LSA to its neighbor, it keeps the LSA until it receives back the acknowledgment message. If the router receives no acknowledgment, it will resend the LSA.

The setting of the restransmit-interval parameter should be conservative, or needless retransmission will result. The value should be larger for serial lines and virtual links.

Examples

The following example sets the retransmit interval value to 8 seconds:

```
Router(config)# interface ethernet0/0
Router(config-if)# ospfv3 101 retransmit-interval 8
```

Related Commands

Command	Description
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

ospfv3 transmit-delay

To set the estimated time required to send a link-state update packet on the Open Shortest Path First version 3 (OSPFv3) interface, use the **ospfv3 transmit-delay** command in interface configuration mode. To return to the default value, use the **no** form of this command.

ospfv3 [*process-id*] **transmit-delay** *seconds*

no ospfv3 [*process-id*] **transmit-delay** *seconds*

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the Open Shortest Path First version 3 (OSPFv3) routing process and can be a value from 1 through 65535.
seconds	Time (in seconds) required to send a link-state update. The range is from 1 to 65535 seconds. The default is 1 second.

Command Default

The default is 1 second.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

Use the **ospfv3 transmit-delay** command to set the estimated time required to send a link-state update packet on the interface. When the **ospfv3 transmit-delay** command is configured with the *process-id* argument, it overwrites the **ipv6 ospf transmit-delay** configuration if OSPFv3 was attached to the interface using the **ipv6 ospf area** command. When the **ospfv3 transmit-delay** command is configured without the *process-id* argument, it is inherited on all instances running on the interface.

Link-state advertisements (LSAs) in the update packet must have their ages incremented by the amount specified in the *seconds* argument before transmission. The value assigned should take into account the transmission and propagation delays for the interface.

If the delay is not added before transmission over a link, the time in which the LSA propagates over the link is not considered. This setting has more significance on very low-speed links.

Examples

The following example sets the retransmit delay value to 3 seconds:

```
Router(config)# interface ethernet0/0
Router(config-if)# ospfv3 101 transmit-delay 3
```

Related Commands

Command	Description
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

other-config-flag

To verify the advertised other configuration parameter, use the **other-config-flag** command in router advertisement (RA) guard policy configuration mode.

other-config-flag {**on** | **off**}

Syntax Description

on	Verification is enabled.
off	Verification is disabled.

Command Default

Verification is not enabled.

Command Modes

RA guard policy configuration (config-ra-guard)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

The **other-config-flag** command enables verification of the advertised "other" configuration parameter (or "O" flag). This flag could be set by an attacker to force hosts to retrieve other configuration information through a potentially untrusted DHCPv6 server.

Examples

The following example defines an RA guard policy name as raguard1, places the router in RA guard policy configuration mode, and enables O flag verification:

```
Router(config)# ipv6 nd raguard policy raguard1
Router(config-ra-guard)# other-config-flag on
```

Related Commands

Command	Description
ipv6 nd raguard policy	Defines the RA guard policy name and enter RA guard policy configuration mode.

outbound-proxy

To configure a Session Initiation Protocol (SIP) outbound proxy for outgoing SIP messages globally on a Cisco IOS voice gateway, use the **outbound-proxy** command in voice service SIP configuration mode. To globally disable forwarding of SIP messages to a SIP outbound proxy globally, use the **no** form of this command.

outbound-proxy {**dhcp** | **ipv4:***ip-address*[**:***port-number*] | **dns:***host***:***domain* [**reuse**]}

no outbound-proxy

Syntax Description

dhcp	Specifies the SIP outbound proxy globally for a Cisco IOS voice gateway; all SIP dialog-initiating requests are sent to the SIP server obtained via DHCP.
ipv4:*ip-address*	Specifies the SIP outbound proxy globally for a Cisco IOS voice gateway; all SIP dialog-initiating requests are sent to this IP address. The colon is required.
:*port-number*	(Optional) The port to which all SIP dialog-initiating requests are sent at the specified IP address. Port number ranges from 0 to 65535. The default is 5060. The colon is required.
dns:*host***:***domain*	Specifies the SIP outbound proxy globally for a Cisco IOS voice gateway; all initiating requests are sent to the specified destination domain. The colon is required.
reuse	(Optional) Reuses the outbound proxy address established during registration for all subsequent registration refreshes and calls.

Command Default

The Cisco IOS voice gateway does not forward outbound SIP messages to a proxy.

Command Modes

Voice service VoIP SIP configuration (conf-serv-sip)

Command History

Release	Modification
12.4(15)T	This command was introduced.
12.4(22)T	Support for IPv6 was added.
12.4(22)YB	This command was modifed. The **dhcp** keyword was added.
15.0(1)M	This command was integrated in Cisco IOS Release 15.0(1)M.
15.1(2)T	This command was modified. The **reuse** keyword was added.

Usage Guidelines

You can use the **outbound-proxy** command in voice service SIP configuration mode to specify outbound proxy settings globally for a Cisco IOS voice gateway. You can also use the **voice-class sip outbound-proxy** command in dial peer voice configuration mode to configure settings for an individual dial peer that override or defer to the global settings for the gateway. However, if both a Cisco Unified Communications Manager Express (CME) and a SIP gateway are configured on the same router, then there is a scenario that can cause incoming SIP messages from line-side phones to be confused with SIP

messages coming from the network side. To avoid failed calls caused by this scenario, disable the SIP outbound proxy setting for all line-side phones on a dial peer using the **outbound-proxy system** command in voice register global configuration mode.

Examples

The following example shows how to specify the SIP outbound proxy globally for a Cisco IOS voice gateway using an IP address:

```
Router> enable
Router# configure terminal
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# outbound-proxy ipv4:10.1.1.1
```

The following example shows how to specify the SIP outbound proxy globally for a Cisco IOS voice gateway using a destination hostname and domain:

```
Router> enable
Router# configure terminal
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# outbound-proxy dns:sipproxy:example.com
```

The following example shows how to specify the SIP outbound proxy globally for a Cisco IOS voice gateway using the DHCP protocol:

```
Router> enable
Router# configure terminal
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# outbound-proxy dhcp
```

Related Commands

Command	Description
outbound-proxy system	Specifies whether Cisco Unified CME line-side SIP phones use the outbound proxy settings configured globally for a Cisco IOS voice gateway.
voice-class sip outbound-proxy	Configures SIP outbound proxy settings for an individual dial peer that override global settings for the Cisco IOS voice gateway.

parameter-map type inspect

To configure an inspect type parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action, use the **parameter-map type inspect** command in global configuration mode. To delete an inspect type parameter map, use the **no** form of this command.

parameter-map type inspect {*parameter-map-name* | **global** | **default**}

no parameter-map type inspect {*parameter-map-name* | **global** | **default**}

Syntax Description

parameter-map-name	Name of the inspect parameter map.
global	Defines a global inspect parameter map.
default	Defines a default inspect parameter map.

Command Default

No inspect type parameter maps are set.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(6)T	This command was introduced.
15.1(1)T	The keywords **global** and **default** were added.
15.1(2)T	Support for IPv6 was added.

Usage Guidelines

After you enter the **parameter-map type inspect** command, you can enter the following commands in parameter-map type inspect configuration mode:

- **alert** {**on** | **off**}

  Turns on Cisco IOS stateful packet inspection alert messages.

- **audit-trail** {**on** | **off**}

  Turns audit trail messages on or off.

- **dns-timeout** *seconds*

  Specifies the Domain Name System (DNS) idle timeout.

- **icmp idle-timeout** *seconds*

  Configures the timeout for Internet Control Message Protocol (ICMP) sessions.

- **max-incomplete** {**low** | **high**} *number-of-connections*

  Defines the number of existing half-open sessions that will cause the software to start and stop deleting half-open sessions.

- **one-minute** {**low** | **high**} *number-of-connections*

Defines the rate of new half-open session initiation in one minute that will cause the system to start deleting half-open sessions and stop deleting half-open sessions.

- **tcp finwait-time** *seconds*

  Specifies how long a TCP session will be managed after the Cisco IOS firewall detects a FIN-exchange.

- **tcp idle-time** *seconds*

  Configures the timeout for TCP sessions.

- **tcp max-incomplete host** *threshold* [**block-time** *minutes*}

  Specifies threshold and blocking time values for TCP host-specific denial-of-service (DOS) detection and prevention.

- **tcp synwait-time** *seconds*

  Specifies how long the software will wait for a TCP session to reach the established state before dropping the session.

- **udp idle-time** *seconds*

  Configures the timeout of User Datagram Protocol (UDP) sessions going through the firewall.

For more detailed information about these commands, see their individual command descriptions.

Examples

The following example shows a sample inspect parameter map with the Cisco IOS stateful packet inspection alert messages enabled:

```
parameter-map type inspect eng-network-profile
 alert on
```

The following example shows a sample inspect type parameter map configuration:

```
parameter-map type inspect eng_network_profile
 audit-trail on
 alert on
 max-incomplete low unlimited
 max-incomplete high unlimited
 one-minute low unlimited
 one-minute high unlimited
 udp idle-time 30
 icmp idle-time 10
 dns-timeout 5
 tcp idle-time 3600
 tcp finwait-time 5
 tcp synwait-time 30
 tcp block-non-session
 tcp max-incomplete host 1-2147483647 block-time unlimited
 sessions maximum:2147483647
```

Related Commands

Command	Description
alert	Turns on Cisco IOS stateful packet inspection alert messages.
audit-trail	Turns audit trail messages on and off.
dns-timeout	Specifies the DNS idle timeout.
icmp idle-timeout	Configures the timeout for ICMP sessions.

Command	Description
inspect	Enables Cisco IOS stateful packet inspection.
max-incomplete	Defines the number of existing half-open sessions that will cause the software to start and stop deleting half-open sessions.
one-minute	Defines the number of new unestablished sessions that will cause the system to start deleting half-open sessions and stop deleting half-open sessions.
ipv6 routing-enforcement-header loose	Provides backward compatibility with legacy IPv6 inspection.
tcp finwait-time	Specifies how long a TCP session will be managed after the Cisco IOS firewall detects a FIN-exchange.
tcp idle-time	Configures the timeout for TCP sessions.
tcp max-incomplete host	Specifies threshold and blocking time values for TCP host-specific denial-of-service (DOS) detection and prevention.
tcp synwait-time	Specifies how long the software will wait for a TCP session to reach the established state before dropping the session.
udp idle-time	Configures the timeout of UDP sessions going through the firewall.

passive-interface (IPv6)

To disable sending routing updates on an interface, use the **passive-interface** command in router configuration mode. To reenable the sending of routing updates, use the **no** form of this command.

passive-interface [**default** | *interface-type interface-number*]

no passive-interface [**default** | *interface-type interface-number*]

Syntax Description

default	(Optional) All interfaces become passive.
interface-type interface-number	(Optional) Interface type and number. For more information, use the question mark (**?**) online help function.

Command Default

No interfaces are passive. Routing updates are sent to all interfaces on which the routing protocol is enabled.

Command Modes

Router configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.4(6)T	Support for Enhanced Internal Gateway Routing Protocol (EIGRP) IPv6 was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

If you disable the sending of routing updates on an interface, the particular address prefix will continue to be advertised to other interfaces, and updates from other routers on that interface continue to be received and processed.

The **default** keyword sets all interfaces as passive by default. You can then configure individual interfaces where adjacencies are desired using the **no passive-interface** command. The **default** keyword is useful in Internet service provider (ISP) and large enterprise networks where many of the distribution routers have more than 200 interfaces.

OSPF for IPv6 routing information is neither sent nor received through the specified router interface. The specified interface address appears as a stub network in the OSPF for IPv6 domain.

For the Intermediate System-to-Intermediate System (IS-IS) protocol, this command instructs IS-IS to advertise the IP addresses for the specified interface without actually running IS-IS on that interface. The **no** form of this command for IS-IS disables advertising IP addresses for the specified address.

Examples

The following example sets all interfaces as passive, then activates Ethernet interface 0:

```
Router(config-router)# passive-interface default
Router(config-router)# no passive-interface ethernet0/0
```

passive-interface (OSPFv3)

To suppress sending routing updates on an interface when using an IPv4 Open Shortest Path First version 3 (OSPFv3) process, use the **passive-interface** command in router configuration mode. To reenable the sending of routing updates, use the **no** form of this command.

passive-interface [**default** | *interface-type interface-number*]

no passive-interface [**default** | *interface-type interface-number*]

Syntax Description

default	(Optional) All interfaces become passive.
interface-type interface-number	(Optional) Interface type and number. For more information, use the question mark (**?**) online help function.

Command Default

No interfaces are passive. Routing updates are sent to all interfaces on which the routing protocol is enabled.

Command Modes

OSPFv3 router configuration mode (config-router)

Command History

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

Usage Guidelines

If you suppress the sending of routing updates on an interface, the particular address prefix will continue to be advertised to other interfaces, and updates from other routers on that interface continue to be received and processed.

The **default** keyword sets all interfaces as passive by default. You can then configure individual interfaces where adjacencies are desired using the **no passive-interface** command. The **default** keyword is useful in Internet service provider (ISP) and large enterprise networks where many of the distribution routers have more than 200 interfaces.

Examples

The following example sets all interfaces as passive, then activates Ethernet interface 0/0:

```
Router(config-router)# passive-interface default
Router(config-router)# no passive-interface ethernet0/0
```

Related Commands

Command	Description
default (OSPFv3)	Returns an OSPFv3 parameter to its default value.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

password (ca-trustpoint)

To specify the revocation password for the certificate, use the **password** command in ca-trustpoint configuration mode. To erase any stored passwords, use the **no** form of this command.

password *string*

no password

Syntax Description

string	Name of the password.

Defaults

You are prompted for the password during certificate enrollment.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.4(24)T	Support for IPv6 Secure Neighbor Discovery (SeND) was added.

Usage Guidelines

Before you can issue the **password** command, you must enable the **crypto ca trustpoint** command, which declares the certification authority (CA) that your router should use and enters ca-trustpoint configuration mode.

This command allows you to specify the revocation password for the certificate before actual certificate enrollment begins. The specified password is encrypted when the updated configuration is written to NVRAM by the router.

If this command is enabled, you will not be prompted for a password during certificate enrollment.

Examples

The following example shows how to specify the password “revokeme” for the certificate request:

```
crypto ca trustpoint trustpoint1
 enrollment url http://trustpoint1.example.com/
 subject-name OU=Spiral Dept., O=example1.com
 ip-address ethernet-0
 auto-enroll regenerate
 password revokeme
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.

peer default ipv6 address pool

To specify the pool from which client prefixes are assigned, use the **peer default ipv6 address pool** command in interface configuration mode. To disable a prior peer IPv6 address pooling configuration on an interface, or to remove the default address from your configuration, use the **no** form of this command.

peer default ipv6 address pool *pool-name*

no peer default ipv6 address pool

Syntax Description

pool-name	Name of a local address pool created using the **ipv6 local pool** command.

Command Default

The default pool name is **pool**.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

This command applies to point-to-point interfaces that support PPP encapsulation. This command sets the address used on the remote (PC) side.

This command allows an administrator to configure all possible address pooling mechanisms on an interface-by-interface basis.

Examples

The following command specifies that this interface will use a local IPv6 address pool named pool3:

```
peer default ipv6 address pool pool3
```

In the following example, the pool1 pool is assigned to virtual template 1:

```
interface Virtual-Template1
 ipv6 enable
 no ipv6 nd suppress-ra
 peer default ipv6 address pool pool1
 ppp authentication chap
```

Related Commands

Command	Description
async dynamic address	Specifies dynamic asynchronous addressing versus default addressing.
encapsulation ppp	Enables PPP encapsulation.
exec	Allows an EXEC process on a line.
ipv6 local pool	Configures a local pool of IPv6 addresses to be used when a remote peer connects to a point-to-point interface.
ppp	Starts an asynchronous connection using PPP.

permit (IPv6)

To set permit conditions for an IPv6 access list, use the **permit** command in IPv6 access list configuration mode. To remove the permit conditions, use the **no** form of this command.

permit *protocol* {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**reflect** *name* [**timeout** *value*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]

no permit {*protocol*} {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**reflect** *name* [**timeout** *value*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]

Internet Control Message Protocol

permit icmp {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [*icmp-type* [*icmp-code*] | *icmp-message*] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]

Transmission Control Protocol

permit tcp {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [**ack**] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**established**] [**fin**] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**neq** {*port* | *protocol*}] [**psh**] [**range** {*port* | *protocol*}] [**reflect** *name* [**timeout** *value*]] [**routing**] [**routing-type** *routing-number*] [**rst**] [**sequence** *value*] [**syn**] [**time-range** *name*] [**urg**]

User Datagram Protocol

permit udp {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**neq** {*port* | *protocol*}] [**range** {*port* | *protocol*}] [**reflect** *name* [**timeout** *value*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]

Syntax Description

protocol	Name or number of an Internet protocol. It can be one of the keywords **ahp**, **esp**, **icmp**, **ipv6**, **pcp**, **sctp**, **tcp**, or **udp**, or an integer in the range from 0 to 255 representing an IPv6 protocol number.
source-ipv6-prefix/*prefix-length*	The source IPv6 network or class of networks about which to set permit conditions. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
any	An abbreviation for the IPv6 prefix ::/0.
host *source-ipv6-address*	The source IPv6 host address about which to set permit conditions. This *source-ipv6-address* argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
auth	Allows matching traffic against the presence of the authentication header in combination with the specified protocol; that is, TCP or UDP.
operator [*port-number*]	(Optional) Specifies an operand that compares the source or destination ports of the specified protocol. Operands are **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range** (inclusive range). If the operator is positioned after the *source-ipv6-prefix*/*prefix-length* argument, it must match the source port. If the operator is positioned after the *destination-ipv6-prefix*/*prefix-length* argument, it must match the destination port. The **range** operator requires two port numbers. All other operators require one port number. The optional *port-number* argument is a decimal number or the name of a TCP or UDP port. A port number is a number from 0 to 65535. TCP port names can be used only when filtering TCP. UDP port names can be used only when filtering UDP.
destination-ipv6-prefix/*prefix-length*	The destination IPv6 network or class of networks about which to set permit conditions. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
host *destination-ipv6-address*	The destination IPv6 host address about which to set permit conditions. This *destination-ipv6-address* argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
dest-option-type	(Optional) Matches IPv6 packets against the destination extension header within each IPv6 packet header.
doh-number	(Optional) Integer in the range from 0 to 255 representing an IPv6 destination option extension header.
doh-type	(Optional) Destination option header types. The possible destination option header type and its corresponding *doh-number* value are home-address—201.
dscp *value*	(Optional) Matches a differentiated services codepoint value against the traffic class value in the Traffic Class field of each IPv6 packet header. The acceptable range is from 0 to 63.

flow-label *value*	(Optional) Matches a flow label value against the flow label value in the Flow Label field of each IPv6 packet header. The acceptable range is from 0 to 1048575.
fragments	(Optional) Matches non-initial fragmented packets where the fragment extension header contains a non-zero fragment offset. The **fragments** keyword is an option only if the *operator* [*port-number*] arguments are not specified.
log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.) The message includes the access list name and sequence number, whether the packet was permitted; the protocol, whether it was TCP, UDP, ICMP, or a number; and, if appropriate, the source and destination addresses and source and destination port numbers. The message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets permitted in the prior 5-minute interval.
log-input	(Optional) Provides the same function as the **log** keyword, except that the logging message also includes the input interface.
mobility	(mobility) Matches IPv6 packets against the mobility extension header within each IPv6 packet header.
mobility-type	(Optional) Matches IPv6 packets against the mobility-type extension header within each IPv6 packet header. Either the *mh-number* or *mh-type* argument must be used with this keyword.
mh-number	(Optional) Integer in the range from 0 to 255 representing an IPv6 mobility header type.
mh-type	(Optional) Mobility header types. Possible mobility header types and their corresponding *mh-number* value are as follows: • 0—bind-refresh • 1—hoti • 2—coti • 3—hot • 4—cot • 5—bind-update • 6—bind-acknowledgment • 7—bind-error
reflect *name*	(Optional) Specifies a reflexive IPvì6 access list. Reflexive IPv6 access lists are created dynamically when an IPv6 packets matches a permit statement that contains the **reflect** keyword. The reflexive IPv6 access list mirrors the permit statement and times out automatically when no IPv6 packets match the permit statement. Reflexive IPv6 access lists can be applied to the TCP, UDP, SCTP, and ICMP for IPv6 packets.
timeout *value*	(Optional) Interval of idle time (in seconds) after which a reflexive IPv6 access list times out. The acceptable range is from 1 to 4294967295. The default is 180 seconds.
routing	(Optional) Matches source-routed packets against the routing extension header within each IPv6 packet header.

routing-type	(Optional) Matches IPv6 packets against the routing-type extension header within each IPv6 packet header. The *routing-number* argument must be used with this keyword.
routing-number	Integer in the range from 0 to 255 representing an IPv6 routing header type. Possible routing header types and their corresponding *routing-number* value are as follows: • 0—Standard IPv6 routing header • 2—Mobile IPv6 routing header
sequence *value*	(Optional) Specifies the sequence number for the access list statement. The acceptable range is from 1 to 4294967295.
time-range *name*	(Optional) Specifies the time range that applies to the permit statement. The name of the time range and its restrictions are specified by the **time-range** and **absolute** or **periodic** commands, respectively.
icmp-type	(Optional) Specifies an ICMP message type for filtering ICMP packets. ICMP packets can be filtered by ICMP message type. The ICMP message type can be a number from 0 to 255, some of which include the following predefined strings and their corresponding numeric values: • 144—dhaad-request • 145—dhaad-reply • 146—mpd-solicitation • 147—mpd-advertisement
icmp-code	(Optional) Specifies an ICMP message code for filtering ICMP packets. ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code. The code is a number from 0 to 255.
icmp-message	(Optional) Specifies an ICMP message name for filtering ICMP packets. ICMP packets can be filtered by an ICMP message name or ICMP message type and code. The possible names are listed in the "Usage Guidelines" section.
ack	(Optional) For the TCP protocol only: acknowledgment (ACK) bit set.
established	(Optional) For the TCP protocol only: Indicates an established connection. A match occurs if the TCP datagram has the ACK or RST bits set. The nonmatching case is that of the initial TCP datagram to form a connection.
fin	(Optional) For the TCP protocol only: Fin bit set; no more data from sender.
neq {*port* | *protocol*}	(Optional) Matches only packets that are not on a given port number.
psh	(Optional) For the TCP protocol only: Push function bit set.
range {*port* | *protocol*}	(Optional) Matches only packets in the range of port numbers.
rst	(Optional) For the TCP protocol only: Reset bit set.
syn	(Optional) For the TCP protocol only: Synchronize bit set.
urg	(Optional) For the TCP protocol only: Urgent pointer bit set.

Command Default No IPv6 access list is defined.

Command Modes IPv6 access list configuration

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.4(2)T	The *icmp-type* argument was enhanced. The **dest-option-type**, **mobility**, **mobility-type**, and **routing-type** keywords were added. The *doh-number*, *doh-type*, *mh-number*, *mh-type*, and *routing-number* arguments were added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 series routers.
12.4(20)T	The **auth** keyword was added.
12.2(33)SRE	This command was modified. It was implemented into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines The **permit** (IPv6) command is similar to the **permit** (IP) command, except that it is IPv6-specific.

Use the **permit** (IPv6) command following the **ipv6 access-list** command to define the conditions under which a packet passes the access list or to define the access list as a reflexive access list.

Specifying IPv6 for the *protocol* argument matches against the IPv6 header of the packet.

By default, the first statement in an access list is number 10, and the subsequent statements are incremented by 10.

You can add **permit**, **deny**, **remark**, or **evaluate** statements to an existing access list without retyping the entire list. To add a new statement anywhere other than at the end of the list, create a new statement with an appropriate entry number that falls between two existing entry numbers to indicate where it belongs.

In Cisco IOS Release 12.2(2)T or later releases, 12.0(21)ST, and 12.0(22)S, IPv6 access control lists (ACLs) are defined and their deny and permit conditions are set by using the **ipv6 access-list** command with the **deny** and **permit** keywords in global configuration mode. In Cisco IOS Release 12.0(23)S or later releases, IPv6 ACLs are defined by using the **ipv6 access-list** command in global configuration mode and their permit and deny conditions are set by using the **deny** and **permit** commands in IPv6 access list configuration mode. Refer to the **ipv6 access-list** command for more information on defining IPv6 ACLs.

Note In Cisco IOS Release 12.0(23)S or later releases, every IPv6 ACL has implicit **permit icmp any any nd-na**, **permit icmp any any nd-ns**, and **deny ipv6 any any** statements as its last match conditions. (The former two match conditions allow for ICMPv6 neighbor discovery.) An IPv6 ACL must contain at least one entry for the implicit **deny ipv6 any any** statement to take effect.

The IPv6 neighbor discovery process makes use of the IPv6 network layer service; therefore, by default,

IPv6 ACLs implicitly allow IPv6 neighbor discovery packets to be sent and received on an interface. In IPv4, the Address Resolution Protocol (ARP), which is equivalent to the IPv6 neighbor discovery process, makes use of a separate data link layer protocol; therefore, by default, IPv4 ACLs implicitly allow ARP packets to be sent and received on an interface.

Both the *source-ipv6-prefix*/*prefix-length* and *destination-ipv6-prefix*/*prefix-length* arguments are used for traffic filtering (the source prefix filters traffic based upon the traffic source; the destination prefix filters traffic based upon the traffic destination).

Note IPv6 prefix lists, not access lists, should be used for filtering routing protocol prefixes.

The **fragments** keyword is an option only if the *operator* [*port-number*] arguments are not specified.

The following is a list of ICMP message names:

- beyond-scope
- destination-unreachable
- echo-reply
- echo-request
- header
- hop-limit
- mld-query
- mld-reduction
- mld-report
- nd-na
- nd-ns
- next-header
- no-admin
- no-route
- packet-too-big
- parameter-option
- parameter-problem
- port-unreachable
- reassembly-timeout
- renum-command
- renum-result
- renum-seq-number
- router-advertisement
- router-renumbering
- router-solicitation
- time-exceeded
- unreachable

Defining Reflexive Access Lists

To define an IPv6 reflexive list, a form of session filtering, use the **reflect** keyword in the **permit** (IPv6) command. The **reflect** keyword creates an IPv6 reflexive access list and triggers the creation of entries in the reflexive access list. The **reflect** keyword must be an entry (condition statement) in an IPv6 access list.

Note For IPv6 reflexive access lists to work, you must nest the reflexive access list using the **evaluate** command.

If you are configuring IPv6 reflexive access lists for an external interface, the IPv6 access list should be one that is applied to outbound traffic.

If you are configuring an IPv6 reflexive access list for an internal interface, the IPv6 access list should be one that is applied to inbound traffic.

IPv6 sessions that originate from within your network are initiated with a packet exiting your network. When such a packet is evaluated against the statements in the IPv6 access list, the packet is also evaluated against the IPv6 reflexive permit entry.

As with all IPv6 access list entries, the order of entries is important, because they are evaluated in sequential order. When an IPv6 packet reaches the interface, it will be evaluated sequentially by each entry in the access list until a match occurs.

If the packet matches an entry prior to the reflexive permit entry, the packet will not be evaluated by the reflexive permit entry, and no temporary entry will be created for the reflexive access list (session filtering will not be triggered).

The packet will be evaluated by the reflexive permit entry if no other match occurs first. Then, if the packet matches the protocol specified in the reflexive permit entry, the packet is forwarded and a corresponding temporary entry is created in the reflexive access list (unless the corresponding entry already exists, indicating that the packet belongs to a session in progress). The temporary entry specifies criteria that permit traffic into your network only for the same session.

Characteristics of Reflexive Access List Entries

The **permit** (IPv6) command with the **reflect** keyword enables the creation of temporary entries in the same IPv6 reflexive access list that was defined by the **permit** (IPv6) command. The temporary entries are created when an IPv6 packet exiting your network matches the protocol specified in the **permit** (IPv6) command. (The packet “triggers” the creation of a temporary entry.) These entries have the following characteristics:

- The entry is a permit entry.
- The entry specifies the same IP upper-layer protocol as the original triggering packet.
- The entry specifies the same source and destination addresses as the original triggering packet, except that the addresses are swapped.
- If the original triggering packet is TCP or UDP, the entry specifies the same source and destination port numbers as the original packet, except that the port numbers are swapped.
- If the original triggering packet is a protocol other than TCP or UDP, port numbers do not apply, and other criteria are specified. For example, for ICMP, type numbers are used: The temporary entry specifies the same type number as the original packet (with only one exception: if the original ICMP packet is type 8, the returning ICMP packet must be type 0 to be matched).
- The entry inherits all the values of the original triggering packet, with exceptions only as noted in the previous four bullets.

- IPv6 traffic entering your internal network will be evaluated against the entry, until the entry expires. If an IPv6 packet matches the entry, the packet will be forwarded into your network.
- The entry will expire (be removed) after the last packet of the session is matched.
- If no packets belonging to the session are detected for a configured length of time (the timeout period), the entry will expire.

Examples

The following example configures two IPv6 access lists named OUTBOUND and INBOUND and applies both access lists to outbound and inbound traffic on Ethernet interface 0. The first and second permit entries in the OUTBOUND list permit all TCP and UDP packets from network 2001:ODB8:0300:0201::/64 to exit out of Ethernet interface 0. The entries also configure the temporary IPv6 reflexive access list named REFLECTOUT to filter returning (incoming) TCP and UDP packets on Ethernet interface 0. The first deny entry in the OUTBOUND list keeps all packets from the network FEC0:0:0:0201::/64 (packets that have the site-local prefix FEC0:0:0:0201 as the first 64 bits of their source IPv6 address) from exiting out of Ethernet interface 0. The third permit entry in the OUTBOUND list permits all ICMP packets to exit out of Ethernet interface 0.

The permit entry in the INBOUND list permits all ICMP packets to enter Ethernet interface 0. The **evaluate** command in the list applies the temporary IPv6 reflexive access list named REFLECTOUT to inbound TCP and UDP packets on Ethernet interface 0. When outgoing TCP or UDP packets are permitted on Ethernet interface 0 by the OUTBOUND list, the INBOUND list uses the REFLECTOUT list to match (evaluate) the returning (incoming) TCP and UDP packets. Refer to the **evaluate** command for more information on nesting IPv6 reflexive access lists within IPv6 ACLs.

```
ipv6 access-list OUTBOUND
 permit tcp 2001:0DB8:0300:0201::/64 any reflect REFLECTOUT
 permit udp 2001:0DB8:0300:0201::/64 any reflect REFLECTOUT
 deny FEC0:0:0:0201::/64 any
 permit icmp any any

ipv6 access-list INBOUND
 permit icmp any any
 evaluate REFLECTOUT

interface ethernet 0
 ipv6 traffic-filter OUTBOUND out
 ipv6 traffic-filter INBOUND in
```

Note Given that a **permit any any** statement is not included as the last entry in the OUTBOUND or INBOUND access list, only TCP, UDP, and ICMP packets will be permitted out of and in to Ethernet interface 0 (the implicit deny all condition at the end of the access list denies all other packet types on the interface).

The following example shows how to allow the matching of any UDP traffic. The authentication header may be present.

```
permit udp any any sequence 10
```

The following example shows how to allow the matching of only TCP traffic if the authentication header is also present.

```
permit tcp any any auth sequence 20
```

The following example shows how to allow the matching of any IPv6 traffic where the authentication header is present.

```
permit ahp any any sequence 30
```

Related Commands

Command	Description
ipv6 access-list	Defines an IPv6 access list and enters IPv6 access list configuration mode.
ipv6 traffic-filter	Filters incoming or outgoing IPv6 traffic on an interface.
deny (IPv6)	Sets deny conditions for an IPv6 access list.
evaluate (IPv6)	Nests an IPv6 reflexive access list within an IPv6 access list.
show ipv6 access-list	Displays the contents of all current IPv6 access lists.

ping

To diagnose basic network connectivity on AppleTalk, ATM, Connectionless Network Service (CLNS), DECnet, IP, Novell IPX, or source-route bridging (SRB) networks, use the **ping** command in user EXEC or privileged EXEC mode.

ping [[*protocol* [**tag**] {*host-name* | *system-address*}]

Syntax Description

protocol	(Optional) Protocol keyword, either **appletalk**, **atm**, **clns**, **decnet**, **ipx**, or **srb**. If a protocol is not specified, a basic ping will be sent using IP (IPv4). For extended options for ping over IP, see the documentation for the **ping ip** command. The **ping atm interface atm**, **ping ip**, **ping ipv6**, **ping sna**, and **ping vrf** commands are documented separately.
tag	(Optional) Specifies a tag encapsulated IP (tagIP) ping.
host-name	Hostname of the system to ping. If a *host-name* or *system-address* is not specified at the command line, it will be required in the **ping** system dialog.
system-address	Address of the system to ping. If a *host-name* or *system-address* is not specified at the command line, it will be required in the **ping** system dialog.

Command Default

This command has no default values.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.0(7)T	The **ping sna** command was introduced.
12.1(12c)E	The **ping vrf** command was introduced.
12.2(2)T	Support for the IPv6 protocol was added.
12.2(13)T	The **atm** protocol keyword was added. The following keywords were removed because the Apollo Domain, Banyan VINES, and XNS protocols are no longer supported in Cisco IOS software: • **apollo** • **vines** • **xns**
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The **ping** command sends an echo request packet to an address then waits for a reply. Ping output can help you evaluate path-to-host reliability, delays over the path, and whether the host can be reached or is functioning. For example, the **ping clns** command sends International Organization for Standardization (ISO) CLNS echo packets to test the reachability of a remote router over a connectionless Open System Interconnection (OSI) network.

If you enter the **ping** command without any keywords or argument values, an interactive system dialog prompts you for the additional syntax appropriate to the protocol you specify. (See the "Examples" section.)

To exit the interactive ping dialog before responding to all the prompts, type the escape sequence. The default escape sequence is **Ctrl**-**^**, **X** (Simultaneously press and release the **Ctrl**, **Shift**, and **6** keys and then press the **X** key). The escape sequence will vary depending on your line configuration. For example, another commonly used escape sequence is **Ctrl**-**c**.

Table 39 describes the test characters sent by the **ping** facility.

Table 39 ping Test Characters

Character	Description
!	Each exclamation point indicates receipt of a reply.
.	Each period indicates that the network server timed out while waiting for a reply.
U	A destination unreachable error protocol data unit (PDU) was received.
C	A reply packet does not validate the reply data, and hence is marked "Corrupted". **Note** This character will only appear if the "validate" option is selected in the ping request.
I	User interrupted test.
M	A destination unreachable error protocol data unit (PDU) was received (Type 3) MTU required but DF bit set (code 4) with the "Next-Hop MTU" set to a non-zero value. If the "Next-hop MTU" is zero then 'U' is printed.
?	Unknown packet type.
&	Packet lifetime exceeded.

Note Not all protocols require hosts to support pings. For some protocols, the pings are Cisco defined and can be answered only by another Cisco router.

The availability of protocol keywords depends on what protocols are enabled on your system.

Issuing the **ping** command in user EXEC mode will generally offer fewer syntax options than issuing the **ping** command in privileged EXEC mode.

Examples

After you enter the **ping** command in privileged EXEC mode, the system prompts you for a protocol keyword. The default protocol is IP.

If you enter a hostname or address on the same line as the **ping** command, the default action is taken as appropriate for the protocol type of that name or address.

The following example is sample dialog from the **ping** command using default values. The specific dialog varies somewhat from protocol to protocol.

```
Router# ping

Protocol [ip]:
Target IP address: 192.168.7.27

Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.7.27, timeout is 2 seconds:
!!!!!
Success rate is 100 percent, round-trip min/avg/max = 1/2/4 ms
```

Table 40 describes the significant fields shown in the display.

Table 40 ping Field Descriptions for IP

Field	Description
Protocol [ip]:	Prompt for a supported protocol. Default: **ip**.
Target IP address:	Prompt for the IP address or hostname of the destination node you plan to ping. If you have specified a supported protocol other than IP, enter an appropriate address for that protocol here. Default: none.
Repeat count [5]:	Number of ping packets that will be sent to the destination address. Default: 5.
Datagram size [100]:	Size of the ping packet (in bytes). Default: 100 bytes.
Timeout in seconds [2]:	Timeout interval. Default: 2 (seconds).
Extended commands [n]:	Specifies whether a series of additional commands appears.
Sweep range of sizes [n]:	Allows you to vary the sizes of the echo packets being sent. This capability is useful for determining the minimum sizes of the maximum transmission units (MTUs) configured on the nodes along the path to the destination address. Packet fragmentation contributing to performance problems can then be reduced.
!!!!!	Each exclamation point (!) indicates receipt of a reply. A period (.) indicates that the network server timed out while waiting for a reply. Other characters may appear in the ping output display, depending on the protocol type.

Table 40 ping Field Descriptions for IP (continued)

Field	Description
Success rate is 100 percent	Percentage of packets successfully echoed back to the router. Anything less than 80 percent is usually considered problematic.
round-trip min/avg/max = 1/2/4 ms	Round-trip travel time intervals for the protocol echo packets, including minimum/average/maximum (in milliseconds).

The following example verifies connectivity to the neighboring ATM device for the ATM permanent virtual circuit (PVC) with the virtual path identifier (VPI)/virtual channel identifier (VCI) value 0/16:

```
Router# ping

Protocol [ip]:atm
ATM Interface:atm1/0
VPI value [0]:
VCI value [1]:16
Loopback - End(0), Segment(1) [0]:1
Repeat Count [5]:
Timeout [2]:
Type escape sequence to abort.
Sending 5, 53-byte segment OAM echoes, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Table 41 describes the default **ping** fields shown in the display.

Table 41 ping Field Descriptions for ATM

Field	Description
Protocol [ip]:	Prompt for a supported protocol. Default: **ip**.
ATM Interface:	Prompt for the ATM interface.
VPI value [0]:	Prompt for the virtual path identifier. Default: 0.
VCI value [1]:	Prompt for the virtual channel identifier. Default:1.
Loopback - End(0), Segment(1) [0]:	Prompt to specify end loopback, which verifies end-to-end PVC integrity, or segment loopback, which verifies PVC integrity to the neighboring ATM device. Default: segment loopback.
Repeat Count [5]:	Number of ping packets that will be sent to the destination address. Default: 5.
Timeout [2]:	Timeout interval. Default: 2 (seconds).
!!!!!	Each exclamation point (!) indicates receipt of a reply. A period (.) indicates that the network server timed out while waiting for a reply. Other characters may appear in the ping output display, depending on the protocol type.

Table 41 ping Field Descriptions for ATM (continued)

Field	Description
Success rate is 100 percent	Percentage of packets successfully echoed back to the router. Anything less than 80 percent is usually considered problematic.
round-trip min/avg/max = 1/1/1 ms	Round-trip travel time intervals for the protocol echo packets, including minimum/average/maximum (in milliseconds).

Related Commands

Command	Description
ping atm interface atm	Tests the connectivity of a specific PVC.
ping ip	Tests network connectivity on IP networks.
ping ipv6	Tests the connection to a remote host on the network using IPv6.
ping sna	Tests network integrity and timing characteristics over an SNA Switching network.
ping vrf	Tests the connection in the context of a specific VPN (VRF).

ping ipv6

To diagnose basic network connectivity when using IPv6, use the **ping IPv6** command in user EXEC or privileged EXEC mode.

ping ipv6 *ipv6-address* [**data** *hex-data-pattern* | **repeat** *repeat-count* | **size** *datagram-size* | **source** [**async** | **bvi** | **ctunnel** | **dialer** | **ethernet** | **fastEthernet** | **gigabitEthernet** | **loopback** | **mfr** | **multilink** | **null** | **port-channel** | **tunnel** | **virtual-template** | *source-address* | **xtagatm**] | **timeout** *seconds* | **verbose**]

Syntax Description

ipv6-address	The address or hostname of the IPv6 host to be pinged. This address or hostname must be in the form documented in RFC 2373, where the address is specified in hexadecimal using 16-bit values between colons.
data	(Optional) Specifies the data pattern.
hex-data-pattern	(Optional) Range is from 0 to FFFF.
repeat	(Optional) Specifies the number of pings sent. The default is 5.
repeat-count	(Optional) Range is from 1 to 2147483647.
size	(Optional) Specifies the datagram size. Datagram size is the number of bytes in each ping.
datagram-size	(Optional) Range is from 48 to 18024.
source	(Optional) Specifies the source address or name.
async	(Optional) Asynchronous interface.
bvi	(Optional) Bridge-Group Virtual Interface.
ctunnel	(Optional) CTunnel interface.
dialer	(Optional) Dialer interface.
ethernet	(Optional) Ethernet IEEE 802.3.
fastEthernet	(Optional) FastEthernet IEEE 802.3.
gigabitEthernet	(Optional) GigabitEthernet IEEE 802.3z.
loopback	(Optional) Loopback interface.
mfr	(Optional) Multilink frame relay (MFR) bundle interface.
multilink	(Optional) Multilink-group interface.
null	(Optional) Null interface.
port-channel	(Optional) Ethernet channel of interfaces.
tunnel	(Optional) Tunnel interface.
virtual-template	(Optional) Virtual template interface.
source-address	(Optional) Source IPv6 address or name.
xtagatm	(Optional) Extended Tag ATM interface.
timeout	(Optional) Specifies the timeout interval in seconds. The default is 2 seconds.
seconds	(Optional) Range is from 0 to 3600.
verbose	(Optional) Displays the verbose output.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The user-level ping feature provides a basic ping facility for users that do not have system privileges. This feature allows the Cisco IOS software to perform the simple default ping functionality for a number of protocols.

The ping program sends an echo request packet to an address, then awaits a reply. Ping output can help you evaluate path-to-host reliability, delays over the path, and whether the host can be reached or is functioning.

If the system cannot map an address for a hostname, it returns an "%Unrecognized host or address, or protocol not running" message.

To abnormally terminate a ping session, type the escape sequence—by default, Ctrl-^ X. You type the default by simultaneously pressing and releasing the Ctrl, Shift, and 6 keys, and then pressing the X key.

Caution When the **timeout** keyword is used with the *seconds* argument set to 0, an immediate timeout occurs, which causes a flood ping. Use the **timeout 0** parameter with caution, because you may receive replies only from immediately adjacent routers depending on router and network use, distance to the remote device, and other factors.

Table 42 describes the characters displayed by the ping facility in IPv6.

Table 42 ping Test Characters (IPv6)

!	Each exclamation point indicates receipt of a reply.
.	Each period indicates that the network server timed out while waiting for a reply.
?	Unknown error.
@	Unreachable for unknown reason.
A	Administratively unreachable. Usually, this output indicates that an access list is blocking traffic.
B	Packet too big.
H	Host unreachable.
N	Network unreachable (beyond scope).

Table 42 ping Test Characters (IPv6) (continued)

P	Port unreachable.
R	Parameter problem.
S	Source address failed ingress/egress policy.
T	Time exceeded.
U	No route to host.
X	Reject route to destination.

Note Not all protocols require hosts to support pings. For some protocols, the pings are Cisco-defined and are answered only by another Cisco router.

When the **ping ipv6** command is enabled, the router attempts to resolve hostnames into IPv6 addresses before trying to resolve them into IPv4 addresses, so if a hostname resolves to both an IPv6 and an IPv4 address and you specifically want to use the IPv4 address, use the **ping** (IPv4) command.

Examples

The following user EXEC example shows sample output for the **ping ipv6** command:

```
Router# ping ipv6 2001:0DB8::3/64

Target IPv6 address: 2001:0DB8::3/64
Repeat count [5]:
Datagram size [100]:48
Timeout in seconds [2]:
Extended commands? [no]: yes
UDP protocol? [no]:
Verbose? [no]:
Precedence [0]:
DSCP [0]:
Include hop by hop option? [no]:yes
Include destination option? [no]:y
% Using size of 64 to accommodate extension headers
Sweep range of sizes? [no]:y
Sweep min size [100]: 100
Sweep max size [18024]: 150
Sweep interval [1]: 5
Sending 55, [100..150]-byte ICMP Echos to 2001:0DB8::3/64, timeout is 2 seconds:
Success rate is 100 percent
round-trip min/avg/max = 2/5/10 ms
```

Table 43 describes the default **ping ipv6** fields shown in the display.

Table 43 ping ipv6 Field Descriptions

Field	Description
Target IPv6 address:	Prompts for the IPv6 address or host name of the destination node you plan to ping. Default: none.
Repeat count [5]:	Number of ping packets that will be sent to the destination address. Default: 5.
Datagram size [100]:	Size of the ping packet (in bytes). Default: 100 bytes.

Table 43 ping ipv6 Field Descriptions (continued)

Field	Description
Timeout in seconds [2]:	Timeout interval (in seconds). Default: 2.
Extended commands [no]:	Specifies whether a series of additional commands appears. Default: no. In an IPv6 dialog for the **ping IPv6** command, entering yes in the Extended commands field displays the UDP protocol?, Verbose, Priority, and Include extension headers? fields.
UDP protocol? [no]:	Specifies UDP packets or ICMPv6 packets. Default: no (ICMP packets are sent).
Verbose? [no]:	Enables verbose output.
Precedence [0]:	Sets precedence in the IPv6 header. The range is from 0 to 7.
DSCP [0]:	Sets Dynamic Host Configuration Protocol (DSCP) in the IPv6 header. The range is from 0 to 63. DSCP appears only if the precedence option is not set, because precedence and DSCP are two separate ways of viewing the same bits in the header.
Include hop by hop option? [no]:	The IPv6 hop-by-hop option is included in the outgoing echo request header, requiring the ping packet to be examined by each node along the path and therefore not be fast-switched or Cisco Express Forwarding-switched. This function may help with debugging network connectivity, especially switching problems. **Note** A Cisco router also includes the hop-by-hop option in the returned echo reply, so the packets should be process-switched rather than fast-switched or Cisco Express Forwarding-switched on the return path also. Non-Cisco routers likely do not have this option in their echo reply; therefore, if the echo request with hop-by-hop option arrives at the destination but the echo reply does not come back and the destination is not a Cisco router, a fast-path issue may exist in an intermediate router.
Include destination option? [no]:	Includes an IPv6 destination option in the outgoing echo request header.
Sweep range of sizes? [no]:	Allows you to vary the sizes of the echo packets being sent. This capability is useful for determining the minimum sizes of the maximum transmission units (MTUs) configured on the nodes along the path to the destination address. Packet fragmentation contributing to performance problems can then be reduced.
Sweep min size [100]: Sweep max size [18024]: Sweep interval [1]:	Options that appear if "Sweep range of sizes?" option is enabled. • Sweep min size—Defaults to the configured "Datagram size" parameter and will override that value if specified. • Sweep Interval—The size of the intervals between the "Sweep min size" and "Sweep max size" parameters. For example, min of 100 max of 150 with an interval of 5 means packets sent are of 100, 105, 110, ..., 150 bytes in size.

Table 43 ping ipv6 Field Descriptions (continued)

Field	Description
Sending 55, [100..150]-byte ICMP Echos to ...	Minimum and maximum sizes and interval as configured in "Sweep range of sizes" options. Sizes are reported if the ping fails (but not if it succeeds, unless the verbose option is enabled).
Success rate is 100 percent	Percentage of packets successfully echoed back to the router. Anything less than 80 percent is usually considered problematic.
round-trip min/avg/max = 2/5/10 ms	Round-trip minimum, average, and maximum time intervals for the protocol echo packets (in milliseconds).

ping vrf

To test a connection in the context of a specific VPN connection, use the **ping vrf** command in user EXEC or privileged EXEC mode.

ping vrf *vrf-name* [**tag**] [*connection*] *target-address* [*connection-options*]

Syntax Description

vrf-name	The name of the VPN (VRF context).
tag	(Optional) Specifies a tag encapsulated IP (tagIP) ping.
connection	(Optional) Connection options include **atm**, **clns**, **decnet**, **ip**, **ipv6**, **ipx**, **sna**, or **srb**. The default is **ip**.
target-address	The destination ID for the ping operation. Usually, this is the IPv4 address of the host. For example, the target for an IPv4 ping in a VRF context would be the IPv4 address or domain name of the target host. The target for an IPv6 ping in a VRF context would be the IPv6 prefix or domain name of the target host. • If the target address is not specified, the CLI will enter the interactive dialog for ping.
connection-options	(Optional) Each connection type may have its own set of connection options. For example, connection options for IPv4 are **source**, **df-bit**, and **timeout**. See the appropriate **ping** command documentation for details.

Command Default

The default connection type for ping is IPv4.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.1(12c)E, 12.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

A VPN routing and forwarding (VRF) instance is used to identify a VPN. To check if a configured VRF is working, you can use the **ping vrf** command.

When attempting to ping from a provider edge (PE) router to a customer edge (CE) router, or from a PE router to PE router, the standard **ping** command will not usually work. The **ping vrf** command allows you to ping the IP addresses of LAN interfaces on CE routers.

If you are on a PE router, be sure to indicate the specific VRF (VPN) name, as shown in the "Examples" section.

If all required information is not provided at the command line, the system will enter the interactive dialog (extended mode) for ping.

Examples

In the following example, the target host in the domain 209.165.201.1 is pinged (using IP/ICMP) in the context of the "CustomerA" VPN connection.

```
Router# ping vrf CustomerA 209.165.201.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.201.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 176/264/576 ms
```

Pressing the Enter key before providing all of the required options will begin the interactive dialog for ping. In the following example, the interactive dialog is started after the "ip" protocol is specified, but no address is given:

```
Router# ping vrf CustomerB ip

Target IP address: 209.165.200.225
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface:
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]: Record
Number of hops [ 9 ]:
Loose, Strict, Record, Timestamp, Verbose[RV]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.225, timeout is 2 seconds:
Packet has IP options:  Total option bytes= 39, padded length=40
 Record route: <*>
   (0.0.0.0)
   (0.0.0.0)
   (0.0.0.0)
   (0.0.0.0)
   (0.0.0.0)
   (0.0.0.0)
   (0.0.0.0)
   (0.0.0.0)
   (0.0.0.0)
 .
 .
 .
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
```

The following example shows the various options for IP in the **ping vrf** command:

```
Router# show parser dump exec | include ping vrf

1 ping vrf <string>
1 ping vrf <string> ip <string>
1 ping vrf <string> ip (interactive)
1 ping vrf <string> ip <string>
1 ping vrf <string> ip <string> source <address>
1 ping vrf <string> ip <string> source <interface>
1 ping vrf <string> ip <string> repeat <1-2147483647>
```

```
1 ping vrf <string> ip <string> size Number
1 ping vrf <string> ip <string> df-bit
1 ping vrf <string> ip <string> validate
1 ping vrf <string> ip <string> data <0-65535>
1 ping vrf <string> ip <string> timeout <0-3600>
1 ping vrf <string> ip <string> verbose
1 ping vrf <string> ip <string> data <0-65535>
1 ping vrf <string> ip <string> timeout <0-3600>
1 ping vrf <string> tag
1 ping vrf <string> atm
1 ping vrf <string> ipv6
1 ping vrf <string> appletalk
1 ping vrf <string> decnet
1 ping vrf <string> clns
1 ping vrf <string> ipx
1 ping vrf <string> sna
1 ping vrf <string> srb
```

Related Commands

Command	Description
ping	Diagnoses basic network connectivity to a specific host.
ping atm interface atm	Tests the connectivity of a specific PVC.
ping ip	Tests the connection to a remote host on the network using IPv4.
ping ipv6	Tests the connection to a remote host on the network using IPv6.
ping sna	Tests network integrity and timing characteristics over an SNA Switching network.

platform ipv6 acl fragment hardware

To permit or deny fragments at hardware, use the **platform ipv6 acl fragment hardware** command in global configuration mode. To reset the IPv6 fragment handling to bridged mode, use the **no** form of this command.

platform ipv6 acl fragment hardware {**forward** | **drop**}

no platform ipv6 acl fragment hardware {**forward** | **drop**}

Syntax Description

forward	Forwards the IPv6 fragments in the hardware.
drop	Drops the IPv6 fragments in the hardware.

Command Default

The **no** form of this command is the default behavior.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.

Usage Guidelines

The PFC3A, PFC3B, and PFC3BXL are unable to handle IPv6 fragments in hardware, and all IPv6 fragments are handled in software. This could result in high CPU if your traffic includes a large amount of IPv6 fragments. This limitation is handled in the PFC3C hardware. The **platform ipv6 acl fragment hardware** command provides a software workaround for the PFC3A, PFC3B, and PFC3BXL by specifying either to permit or drop all IPv6 fragments in hardware.

Note When you enter the **drop** keyword, a small portion of the packets is leaked to the software (for ICMP message generation) and forwarded in software.

The **platform ipv6 acl fragment hardware** command overrides the following actions:

- Any ACE in the IPv6 filter (ACL) that contains the **fragment** keyword. If the ACE in the ACL contains the **fragment** keyword, the associated action (**permit** | **deny** | **log**) is not taken, and the action (**permit** | **drop**) specified by the **platform ipv6 acl fragment hardware** command is taken.
- Any IPv6 ACL that contains ACEs that implicitly permit IPv6 fragments; for example, permit ACEs that contain Layer 4 ports to implicitly permit fragments only.
- If the IPv6 fragment hits the implicit **deny any any** ACE added at the end of the ACL, the IPv6 fragment will not get hit.

Examples

This example shows how to forward the IPv6 fragments at hardware:

```
Router(config)# platform ipv6 acl fragment hardware forward
```

This example shows how to drop the IPv6 fragments at hardware:

```
Router(config)# platform ipv6 acl fragment hardware drop
```

platform ipv6 acl icmp optimize neighbor-discovery

To optimize ternary content addressable memory (TCAM) support for IPv6 access lists (ACLs), use the **platform ipv6 acl icmp optimize neighbor-discovery** command in global configuration mode. To disable optimization of TCAM support for IPv6 ACLs, use the **no** form of this command.

platform ipv6 acl icmp optimize neighbor-discovery

no platform ipv6 acl icmp optimize neighbor-discovery

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	This command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Note Use this command under the direction of the Cisco Technical Assistance Center only.

When you enable optimization of the TCAM support for IPv6 ACLs, the global Internet Control Message Protocol version 6 (ICMPv6) neighbor-discovery ACL at the top of the TCAM is programmed to permit all ICMPv6 neighbor-discovery packets. Enabling optimization prevents the addition of ICMPv6 access control entries (ACEs) at the end of every IPv6 security ACL, reducing the number of TCAM resources being used. Enabling this command reprograms IPv6 ACLs on all interfaces.

Note The ICMPv6 neighbor-discovery ACL at the top of the TCAM takes precedence over security ACLs for ICMP neighbor-discovery packets that you have configured, but has no effect if you have a bridge/deny that overlaps with the global ICMP ACL.

Examples

This example shows how to optimize TCAM support for IPv6 ACLs:

```
Router(config)# platform ipv6 acl icmp optimize neighbor-discovery
```

This example shows how to disable optimization of TCAM support for IPv6 ACLs:

```
Router(config)# no platform ipv6 acl icmp optimize neighbor-discovery
```

platform ipv6 acl punt extension-header

To enable processing of IPv6 packets with extension headers in software on the RP, use the **platform ipv6 acl punt extension-header** command in global configuration mode. To disable processing of IPv6 packets with extension headers in software on the RP, use the **no** form of this command.

platform ipv6 acl punt extension-header

no platform ipv6 acl punt extension-header

Syntax Description

This command has no arguments or keywords.

Command Default

IPv6 packets with extension headers are processed in software.

Command Modes

Global configuration mode

Command History

Release	Modification
12.2(33)SXH7	This command was introduced on the Supervisor Engine 720.

Usage Guidelines

If your IPv6 traffic does not specify a Layer 4 protocol, software processing of IPv6 packets with extension headers is unnecessary. If your IPv6 traffic specifies a Layer 4 protocol, you can enter the **platform ipv6 acl punt extension-header** global configuration command to enable software processing of IPv6 packets with extension headers.

Examples

This example shows how to enable processing of IPv6 packets with extension headers in software on the RP:

```
Router(config)# platform ipv6 acl punt extension-header
Router(config)#
```

This example shows how to disable processing of IPv6 packets with extension headers in software on the RP:

```
Router(config)# no platform ipv6 acl punt extension-header
Router(config)#
```

poison-reverse (IPv6 RIP)

To configure the poison reverse processing of IPv6 Routing Information Protocol (RIP) router updates, use the **poison-reverse** command in router configuration mode. To disable the poison reverse processing of IPv6 RIP updates, use the **no** form of this command.

poison-reverse

no poison-reverse

Syntax Description

This command has no keywords or arguments

Command Default

Poison reverse is not configured.

Command Modes

Router configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

This command configures poison reverse processing of IPv6 RIP router updates. When poison reverse is configured, routes learned via RIP are advertised out the interface over which they were learned, but with an unreachable metric.

If both poison reverse and split horizon are configured, then simple split horizon behavior (suppression of routes out of the interface over which they were learned) is replaced by poison reverse behavior.

Examples

The following example configures poison reverse processing for the IPv6 RIP routing process named cisco:

```
Router(config)# ipv6 router rip cisco
Router(config-rtr)# poison-reverse
```

Related Commands

Command	Description
split-horizon (IPv6 RIP)	Configures split horizon processing of IPv6 RIP router updates.

policy-map type inspect

To create a Layer 3 and Layer 4 or a Layer 7 (protocol-specific) inspect type policy map, use the **policy-map type inspect** command in global configuration mode. To delete an inspect type policy map, use the **no** form of this command.

Layer 3 and Layer 4 (Top Level) Policy Map Syntax

policy-map type inspect *policy-map-name*

no policy-map type inspect *policy-map-name*

Layer 7 (Application-Specific) Policy Map Syntax

policy-map type inspect *protocol-name policy-map-name*

no policy-map type inspect *protocol-name policy-map-name*

Syntax Description

policy-map-name	Name of the policy map. The name can be a maximum of 40 alphanumeric characters.
protocol-name	Layer 7 application-specific policy map. The supported protocols are as follows: • **h323**—H.323 protocol, Version 4 • **http**—HTTP • **im**—Instant Messenger (IM) protocol For **im**, the supported IM protocols include: – AOL Version 5 and later versions – I Seek You (ICQ) Version 2003b.5.56.1.3916.85 – MSN Messenger Version 6.x and 7.x – Windows Messenger Version 5.1.0701 – Yahoo Messenger Version 9.0 and later versions • **imap**—Internet Message Access Protocol (IMAP) • **p2p**—Peer-to-peer (P2P) protocol • **pop3**—Post Office Protocol, Version 3 (POP3) • **sip**—Session Initiation Protocol (SIP) • **smtp**—Simple Mail Transfer Protocol (SMTP) • **sunrpc**—Sun Remote Procedure Call (SUNRPC)

Command Default

No policy-map is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(9)T	Support for the following protocols and keywords was added: • P2P protocol and the **p2p** keyword • IM protocol and the **im** keyword
12.4(15)XZ	This command was integrated into Cisco IOS Release 12.4(15)XZ. Support for the SIP protocol was added.
12.4(20)T	Support for the ICQ and Windows Messenger IM protocols and following keywords was added: **icq**, **winmsgr** Support for the H.323 VoIP protocol and following keyword was added: **h323**
15.1(2)T	Support for IPv6 was added.

Usage Guidelines

Use the **policy-map type inspect** command to create a Layer 3, Layer 4 inspect type policy map or a Layer 7 application-specific inspect type policy map. After you create a policy map, you should enter the **class type inspect** command (as appropriate for your configuration) to specify the traffic (class) on which an action is to be performed. The class was previously defined in a class map. Thereafter, you should enter the **inspect** command to enable Cisco IOS stateful packet inspection and to specify inspect-specific parameters in a parameter map.

Layer 3, Layer 4 (Top Level) Policy Maps

Top-level policy maps allow you to define high-level actions such as **inspect**, **drop**, **pass**, and **urlfilter**. You can attach the maps to a target (zone pair). The maps can contain "child" policies that are also known as application-specific Layer 7 policies.

Layer 7 (Application-Specific) Policy Maps

Application-specific policy maps are used to specify a policy for an application protocol. For example, if you want to drop HTTP traffic with Uniform Resource Identifier (URI) lengths exceeding 256 bytes, you must configure an HTTP policy map to do that. Application-specific policy maps cannot be attached directly to a target (zone pair). They must be configured as "child" policies in a top-level Layer 3 or Layer 4 policy map.

Examples

The following example specifies the traffic class (host) on which the drop action is to be performed:

```
policy-map type inspect mypolicy
 class type inspect host
 drop
```

The following example shows how to configure the policy map "my-im-pmap" with two IM classes—AOL and Yahoo Messenger—and allow only text-chat messages to pass through. When any packet with a service other than "text-chat" is seen, the connection will be reset.

```
class-map type inspect aol match-any my-aol-cmap
 match service text-chat
!
class-map type inspect ymsgr match-any my-ysmgr-cmap
 match service any
!
policy-map type inspect im my-im-pmap
```

```
 class type inspect aol my-aol-cmap
 allow
 log
!
 class type inspect ymsgr my-ysmgr-cmap
 reset
 log
```

Related Commands

Command	Description
class type inspect	Specifies the traffic (class) on which an action is to be performed.

port (dial peer)

To associate a dial peer with a specific voice port, use the **port** command in dial peer configuration mode. To cancel this association, use the **no** form of this command.

Cisco 1750 and Cisco 3700 Series

port *slot-number*/*port*

no port *slot-number*/*port*

Cisco 2600 Series, Cisco 3600 Series, and Cisco 7200 Series

port {*slot-number*/*subunit-number*/*port* | *slot*/*port*:*ds0-group-number*}

no port {*slot-number*/*subunit-number*/*port* | *slot*/*port*:*ds0-group-number*}

Cisco AS5300 and Cisco AS5800

port *controller-number*:**D**

no port *controller-number*:**D**

Cisco uBR92x Series

port *slot*/*subunit*/*port*

no port *slot*/*subunit*/*port*

Syntax Description

Cisco 1750 and Cisco 3700 Series

slot-number	Number of the slot in the router in which the voice interface card (VIC) is installed. Valid entries are from 0 to 2, depending on the slot in which the VIC has been installed.
port	Voice port number. Valid entries are 0 and 1.

Cisco 2600 Series, Cisco 3600 Series, and Cisco 7200 Series

slot-number	Number of the slot in the router in which the VIC is installed. Valid entries are from 0 to 3, depending on the slot in which it has been installed.
subunit-number	Subunit on the VIC in which the voice port is located. Valid entries are 0 and 1.
port	Voice port number. Valid entries are 0 and 1.
slot	Router location in which the voice port adapter is installed. Valid entries are 0 and 3.
port	Voice interface card location. Valid entries are 0 and 3.
ds0-group-number	The DS0 group number. Each defined DS0 group number is represented on a separate voice port. This allows you to define individual DS0s on the digital T1/E1 card.

Cisco AS5300

controller-number	The T1 or E1 controller.
:D	Indicates the D channel associated with the ISDN PRI.

Cisco uBR92x series

slot/*subunit*/*port*	The analog voice port. Valid entries for the *slot*/*subunit*/*port* are as follows: • *slot*—A router slot in which a voice network module (NM) is installed. Valid entries are router slot numbers for the particular platform. • *subunit*—A VIC in which the voice port is located. Valid entries are 0 and 1. (The VIC fits into the voice network module.) • *port*—An analog voice port number. Valid entries are 0 and 1.

Command Default

No port is configured.

Command Modes

Dial peer configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
11.3(3)T	This command was implemented on the Cisco 2600 series.
11.3(1)MA	This command was implemented on the Cisco MC3810.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T and implemented on the Cisco AS5300.
12.0(4)T	This command was implemented on the Cisco uBR924.
12.0(7)T	This command was implemented on the Cisco AS5800.
12.2(8)T	This command was implemented on the following platforms: Cisco 1751, Cisco 3725, and Cisco 3745.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T. This command does not support the extended echo canceller (EC) feature on the Cisco AS5300 or the Cisco AS5800.
12.4(22)T	Support for IPv6 was added.

Usage Guidelines

This command enables calls that come from a telephony interface to select an incoming dial peer and for calls that come from the VoIP network to match a port with the selected outgoing dial peer.

This command applies only to POTS peers.

Note This command does not support the extended EC feature on the Cisco AS5300.

Examples

The following example associates POTS dial peer 10 with voice port 1, which is located on subunit 0 and accessed through port 0:

```
dial-peer voice 10 pots
 port 1/0/0
```

The following example associates POTS dial peer 10 with voice port 0:D:

```
dial-peer voice 10 pots
 port 0:D
```

The following example associates POTS dial peer 10 with voice port 1/0/0:D (T1 card):

```
dial-peer voice 10 pots
 port 1/0/0:D
```

Related Commands

Command	Description
prefix	Specifies the prefix of the dialed digits for a dial peer.

port (IPv6 RIP)

To configure a specified User Datagram Protocol (UDP) port and multicast address for an IPv6 Routing Information Protocol (RIP) routing process, use the **port** command in router configuration mode. To return the port number and multicast address to their default values, use the **no** form of this command.

port *port-number* **multicast-group** *multicast-address*

no port *port-number* **multicast-group** *multicast-address*

Syntax Description

port-number	The UDP port number. Can be a number from 1 to 65535. Table 44 in the "Usage Guidelines" section lists common UDP services and their port numbers.
multicast-group	Specifies a multicast group.
multicast-address	The address or host name of the multicast group.

Command Default

UDP port 521; multicast address FF02::9

Command Modes

Router configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Two IPv6 RIP routing processes cannot use the same UDP port. If two IPv6 RIP routing processes are configured on the same UDP port, the second process will not start up until the configuration conflict is resolved. Two IPv6 RIP routing processes can use the same multicast address. UDP sources and port numbers are shown in Table 44.

Table 44 Common UDP Services and Their Port Numbers

Service	Port
Domain Name System (DNS)	53
Network File System (NFS)	2049
remote-procedure call (RPC)	111

Table 44 Common UDP Services and Their Port Numbers (continued)

Service	Port
Simple Network Management Protocol (SNMP)	161
Trivial File Transfer Protocol (TFTP)	69

Examples

The following example configures UDP 200 and multicast address FF02::9 for the IPv6 RIP routing process named cisco:

```
Router(config)# ipv6 router rip cisco
Router(config-rtr-rip)# port 200 multicast-group FF02::9
```

port (TACACS+)

To specify the TCP port to be used for TACACS+ connections, use the **port** command in TACACS+ server configuration mode. To remove the TCP port, use the **no** form of this command.

port [*number*]

no port [*number*]

Syntax Description

number	(Optional) Specifies the port where the TACACS+ server receives access-request packets. The range is from 1 to 65535.

Command Default

If no port is configured, port 49 is used.

Command Modes

TACACS+ server configuration (config-server-tacacs)

Command History

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

Usage Guidelines

TCP port 49 is used if the *number* argument is not used when using the **port** command.

Examples

The following example shows how to specify TCP port 12:

```
Router (config)# tacacs server server1
Router(config-server-tacacs)# port 12
```

Related Commands

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

ppp accounting

To enable authentication, authorization, and accounting (AAA) accounting services on the selected interface, use the **ppp accounting** command in interface configuration mode. To disable AAA accounting services, use the **no** form of this command.

ppp accounting {**default** | *listname*}

no ppp accounting

Syntax Description

default	The name of the method list is created with the **aaa accounting** command.
listname	A specified method list.

Command Default

Accounting is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.6	The *listname* argument was added.

Usage Guidelines

After you enable the **aaa accounting** command and define a named accounting method list (or use the default method list), you must apply the defined lists to the appropriate interfaces for accounting services to take place. Use the **ppp accounting** command to apply the specified method lists (or if none is specified, the default method list) to the selected interface.

Examples

The following example enables accounting on asynchronous interface 4 and uses the accounting method list named charlie:

```
interface async 4
 encapsulation ppp
 ppp accounting list1
```

Related Commands

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

ppp authentication

To enable at least one PPP authentication protocol and to specify the order in which the protocols are selected on the interface, use the **ppp authentication** command in interface configuration mode. To disable this authentication, use the **no** form of this command.

ppp authentication {*protocol1* [*protocol2...*]} [**if-needed**] [*list-name* | **default**] [**callin**] [**one-time**] [**optional**]

no ppp authentication

Syntax Description

protocol1 [*protocol2...*]	At least one of the keywords described in Table 45.
if-needed	(Optional) Used with TACACS and extended TACACS. Does not perform Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP) authentication if authentication has already been provided. This option is available only on asynchronous interfaces.
list-name	(Optional) Used with authentication, authorization, and accounting (AAA). Specifies the name of a list of methods of authentication to use. If no list name is specified, the system uses the default. The list is created with the **aaa authentication ppp** command.
default	(Optional) Name of the method list created with the **aaa authentication ppp** command.
callin	(Optional) Authentication on incoming (received) calls only.
one-time	(Optional) The username and password are accepted in the username field.
optional	(Optional) Accepts the connection even if the peer refuses to accept the authentication methods that the router has requested.

Defaults

PPP authentication is not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.1(1)	The **optional** keyword was added.
12.1(3)XS	The **optional** keyword was added.
12.2(2)XB5	Support for the **eap** authentication protocol was added on the Cisco 2650, Cisco 3640, Cisco 3660, Cisco AS5300, and Cisco AS5400 platforms.
12.2(13)T	The **eap** authentication protocol support introduced in Cisco IOS Release 12.2(2)XB5 was integrated into Cisco IOS Release 12.2(13)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.5	This command was updated. It was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

When you enable Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), or Extensible Authentication Protocol (EAP) authentication (or all three methods), the local router requires the remote device to prove its identity before allowing data traffic to flow. PAP authentication requires the remote device to send a name and a password, which is checked against a matching entry in the local username database or in the remote security server database. CHAP authentication sends a challenge message to the remote device. The remote device encrypts the challenge value with a shared secret and returns the encrypted value and its name to the local router in a Response message. The local router attempts to match the name of the remote device with an associated secret stored in the local username or remote security server database; it uses the stored secret to encrypt the original challenge and verify that the encrypted values match. EAP works much as CHAP does, except that identity request and response packets are exchanged when EAP starts.

You can enable CHAP, Microsoft CHAP (MS-CHAP), PAP, or EAP in any order. If you enable all four methods, the first method specified is requested during link negotiation. If the peer suggests using the second method, or refuses the first method, the second method is tried. Some remote devices support only one method. Base the order in which you specify methods on the ability of the remote device to correctly negotiate the appropriate method and on the level of data-line security you require. PAP usernames and passwords are sent as clear text strings, which can be intercepted and reused.

Caution If you use a *list-name* value that was not configured with the **aaa authentication ppp** command, you will disable PPP on this interface.

Table 45 lists the protocols used to negotiate PPP authentication.

Table 45 ppp authentication Protocols

chap	Enables CHAP on a serial interface.
eap	Enables EAP on a serial interface.
ms-chap	Enables MS-CHAP on a serial interface.
pap	Enables PAP on a serial interface.

Enabling or disabling PPP authentication does not affect the ability of the local router to authenticate itself to the remote device.

If you are using autoselect on a tty line, you can use the **ppp authentication** command to turn on PPP authentication for the corresponding interface.

MS-CHAP is the Microsoft version of CHAP. Like the standard version of CHAP, MS-CHAP is used for PPP authentication; authentication occurs between a personal computer using Microsoft Windows NT or Microsoft Windows 95 and a Cisco router or access server acting as a network access server.

To configure Cisco PDSN in compliance with the TIA/EIA/IS-835-B standard, you must configure the PDSN virtual template as follows:

```
ppp authentication chap pap optional
```

Examples

The following example configures virtual-template interface 4:

```
interface virtual-template 4
 ip unnumbered loopback0
 ppp authentication chap pap optional
```

The following example enables CHAP on asynchronous interface 4 and uses the authentication list MIS-access:

```
interface async 4
 encapsulation ppp
 ppp authentication chap MIS-access
```

The following example enables EAP on dialer interface 1:

```
interface dialer 1
 encapsulation ppp
 ppp authentication eap
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
aaa new-model	Enables the AAA access control model.
autoselect	Configures a line to start an ARAP, PPP, or SLIP session.
encapsulation	Sets the encapsulation method used by the interface.
ppp accm	Identifies the ACCM table.
username	Establishes a username-based authentication system, such as PPP, CHAP, and PAP.

ppp ipcp

To configure PPP IP Control Protocol (IPCP) features such as the ability to provide primary and secondary Domain Name Server (DNS) and Windows Internet Naming Service (WINS) server addresses, and the ability to accept any address requested by a peer, use the **ppp ipcp** command in template or interface configuration mode. To disable a PPP IPCP feature, use the **no** form of this command.

ppp ipcp {**accept-address** | **address** {**accept** | **required** | **unique**} | **dns** {*primary-ip-address* [*secondary-ip-address*] [**aaa**] [**accept**] | **accept** | **reject** | **request** [**accept**]} | **header-compression ack** | **ignore-map** | **mask** {*subnet-mask* | **reject** | **request**} | **username unique** | **wins** {*primary-ip-address* [*secondary-ip-address*] [**aaa**] [**accept**] | **accept** | **reject** | **request** [**accept**]}}

no ppp ipcp {**accept-address** | **address** {**accept** | **required** | **unique**} | **dns** | **header-compression ack** | **ignore-map** | **mask** | **predictive** | **username unique** | **wins**}

Syntax Description

accept-address	Accepts any nonzero IP address from the peer.
address	Specifies IPCP IP address options: • **accept**—Accepts any nonzero IPv4 or IPv6 address from the peer. • **required**—Disconnects the peer if no IP address is negotiated. • **unique**—Disconnects the peer if the IP address is already in use.
dns	Specifies DNS options: • *primary-ip-address*—IP address of the primary DNS server. – *secondary-ip-address*—(Optional) IP address of the secondary DNS server. – **aaa**—(Optional) Uses DNS data from the AAA server. – **accept**—(Optional) Specifies that any nonzero DNS address will be accepted. • **accept**—Specifies that any nonzero DNS address will be accepted. • **reject**—Rejects the IPCP option if received from the peer. • **request**—Requests the DNS address from the peer.
header-compression ack	Enables IPCP header compression.
ignore-map	Ignores the dialer map when negotiating the peer IP address.
mask	Specifies IP address mask options: • *subnet-mask*—Specifies the subnet mask to offer the peer. • **reject**—Rejects subnet mask negotiations. • **request**—Requests the subnet mask from the peer.

username unique	Ignores a common username when providing an IP address to the peer.
wins	Specifies WINS options: • *primary-ip-address*—IP address of the primary WINS server. – *secondary-ip-address*—(Optional) IP address of the secondary WINS server. – .**aaa**—(Optional) Use WINS data from the AAA server. – **accept**—(Optional) Specifies that any nonzero WINS address will be accepted. • **accept**—Specifies that any nonzero WINS address will be accepted. • **reject**—Reject the IPCP option if received from the peer. • **request**—Request the WINS address from the peer.

Defaults

No servers are configured, and no address request is made.

Command Modes

Template configuration
Interface configuration (config-if)

Command History

Release	Modification
12.0(6)T	This command was introduced.
12.1(5)T	This command was modified. The **reject** and **accept** keywords were added.
Cisco IOS XE Release 3.2S	This command was modified. Support for IPv6 was added.

Examples

The following examples show use of the **ppp ipcp** command:

```
ppp ipcp accept-address

ppp ipcp dns 10.1.1.3

ppp ipcp dns 10.1.1.3 10.1.1.4

ppp ipcp dns 10.1.1.1 10.1.1.2 accept

ppp ipcp dns accept

ppp ipcp dns reject

ppp ipcp ignore-map

ppp ipcp username unique

ppp ipcp wins 10.1.1.1 10.1.1.2

ppp ipcp wins accept
```

The following examples show how to use the **no** form of the **ppp ipcp** command:

```
no ppp ipcp wins

no ppp ipcp ignore-map
```

Related Commands

Command	Description
debug ppp	Displays information on traffic and exchanges in an internetwork implementing the PPP.
show interfaces	Displays statistics for all interfaces configured on the router or access server.
show ip interfaces	Displays the usability status of interfaces configured for IP.

ppp multilink

To enable Multilink PPP (MLP) on an interface and, optionally, to enable Bandwidth Allocation Control Protocol (BACP) and its Bandwidth Allocation Protocol (BAP) subset for dynamic bandwidth allocation, use the **ppp multilink** command in interface configuration mode. To disable Multilink PPP or, optionally, to disable only dynamic bandwidth allocation, use the **no** form of this command.

ppp multilink [**bap**]

no ppp multilink [**bap** [**required**]]

Cisco 10000 Series Router

ppp multilink

no ppp multilink

Syntax Description

bap	(Optional) Specifies bandwidth allocation control negotiation and dynamic allocation of bandwidth on a link.
required	(Optional) Enforces mandatory negotiation of BACP for the multilink bundle. The multilink bundle is disconnected if BACP is not negotiated.

Defaults

This command is disabled. When BACP is enabled, the defaults are to accept calls and to set the timeout pending at 30 seconds.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.1	This command was introduced.
12.0(23)SX	This command was implemented on the Cisco 10000 series router.
12.2(16)BX	This command was implemented on the ESR–PRE2.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

This command applies only to interfaces that use PPP encapsulation.

MLP and PPP reliable links do not work together.

When the **ppp multilink** command is used, the first channel will negotiate the appropriate Network Control Protocol (NCP) layers (such as the IP Control Protocol and IPX Control Protocol), but subsequent links will negotiate only the link control protocol and MLP. NCP layers do not get negotiated on these links, and it is normal to see these layers in a closed state.

This command with the **bap** keyword must be used before configuring any **ppp bap** commands and options. If the **bap required** option is configured and a reject of the options is received, the multilink bundle is torn down.

The **no** form of this command without the **bap** keyword disables both MLP and BACP on the interface.

The **dialer load-threshold** command enables a rotary group to bring up additional links and to add them to a multilink bundle.

Before Cisco IOS Release 11.1, the **dialer-load threshold 1** command kept a multilink bundle of any number of links connected indefinitely, and the **dialer-load threshold 2** command kept a multilink bundle of two links connected indefinitely. If you want a multilink bundle to be connected indefinitely, you must set a very high idle timer.

Note By default, after changing hostnames, an MLP member link does not undergo failure recovery automatically. You must use the **ppp chap hostname** command to define the MLP bundle name on an endpoint. If this command is not configured and the hostname is changed, then a link flap will not return the link back to the bundle.

Cisco 10000 Series Router

The **ppp multilink** command has no arguments or keywords.

Examples

The following partial example shows how to configure a dialer for MLP:

```
interface Dialer0
 ip address 10.0.0.2 255.0.0.0
 encapsulation ppp
 dialer in-band
 dialer idle-timeout 500
 dialer map ip 10.0.0.1 name atlanta broadcast 81012345678901
 dialer load-threshold 30 either
 dialer-group 1
 ppp authentication chap
 ppp multilink
```

Related Commands

Command	Description
compress	Configures compression for LAPB, PPP, and HDLC encapsulations.
dialer fast-idle (interface)	Specifies the idle time before the line is disconnected.
dialer-group	Controls access by configuring an interface to belong to a specific dialing group.
dialer load-threshold	Configures bandwidth on demand by setting the maximum load before the dialer places another call to a destination.
encapsulation ppp	Enables PPP encapsulation.
ppp authentication	Enables CHAP or PAP or both, and specifies the order in which CHAP and PAP authentication is selected on the interface.
ppp bap timeout	Specifies nondefault timeout values for PPP BAP pending actions and responses.
ppp chap hostname	Enables a router calling a collection of routers that do not support this command to configure a common CHAP secret password to use in response to challenges from an unknown peer.

Command	Description
ppp multilink fragment delay	Specifies a maximum time for the transmission of a packet fragment on a MLP bundle.
ppp multilink fragment disable	Disables packet fragmentation.
ppp multilink fragmentation	Sets the maximum number of fragments a packet will be segmented into before being sent over the bundle.
ppp multilink group	Restricts a physical link to joining only a designated multilink-group interface.
ppp multilink interleave	Enables MLP interleaving.
ppp multilink mrru	Configures the MRRU value negotiated on an MLP bundle.
ppp multilink slippage	Defines the constraints that set the MLP reorder buffer size.
show ppp bap	Displays the configuration settings and run-time status for a multilink bundle.

ppp ncp override local

To track attributes received in authorization from RADIUS, verify the permitted Network Control Program (NCP), reject the current NCP negotiation, and override the local dual-stack configuration, use the **ppp ncp override local** command in global configuration mode. To disable the configuration, use the **no** form of this command.

ppp ncp override local

no ppp ncp override local

Syntax Description

This command has no arguments or keywords.

Command Default

The tracking of attributes from RADIUS and the local configuration override are not enabled. The local configuration is used.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

Framed attributes are primarily used for address allocation. The RADIUS server maintains a pool of both IPv4 addresses and IPv6 prefixes. If IPv4 address or IPv6 prefix attributes are absent in the access-accept response from RADIUS, the **ppp ncp override local** command can be used to override local configuration.

Examples

The following example shows how to override the local IPv6 or IPv4 dual-stack configuration:

```
Router> enable
Router# configure terminal
Router(config)# ppp ncp override local
```

ppp timeout ncp

To set a time limit for the successful negotiation of at least one network layer protocol after a PPP connection is established, use the **ppp timeout ncp** command in interface configuration mode. To remove the time limit, use the **no** form of this command.

ppp timeout ncp *seconds*

no ppp timeout ncp

Syntax Description

seconds	Maximum time, in seconds, PPP should wait for negotiation of a network layer protocol. If no network protocol is negotiated in the given time, the connection is disconnected.

Defaults

No time limit is imposed.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.3	This command was introduced as **ppp negotiation-timeout**.
12.2	This command was changed to **ppp timeout ncp**. The **ppp negotiation-timeout** command was accepted by the command line interpreter through Cisco IOS Release 12.2.
Cisco IOS XE Release 3.2S	Support for IPv6 was added.

Usage Guidelines

The **ppp timeout ncp** command protects against the establishment of links that are physically up and carrying traffic at the link level, but are unusable for carrying data traffic due to failure to negotiate the capability to transport any network level data. This command is particularly useful for dialed connections, where it is usually undesirable to leave a telephone circuit active when it cannot carry network traffic.

Examples

The following example sets the Network Control Protocol (NCP) timer to 8 seconds:

```
ppp timeout ncp 8
```

Related Commands

Command	Description
absolute-timeout	Sets the interval for closing user connections on a specific line or port.
dialer idle-timeout (interface)	Specifies the idle time before the line is disconnected.

ppp unique address accept-access

To track duplicate addresses received from RADIUS and create a standalone database, use the **ppp unique address accept-access** command in global configuration mode. To disable this feature and remove the database, use the **no** form of this command.

ppp unique address accept-access

no ppp unique address accept-access

Syntax Description

This command has no arguments or keywords.

Command Default

This feature is not enabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

The **ppp unique address accept-access** command enables the IPv6 router to track and check duplicate attributes received in an Access-Accept response from RADIUS, and triggers creation of a new, standalone database that contains the Access-Accept responses received since the feature was enabled.

The following RADIUS attributes are tracked in this database and checked when an Access-Accept response is received:

- Framed-IP-Address
- Framed-IPv6-Prefix
- Delegated-IPv6-Prefix

All of these RADIUS attributes from this list are checked against the database for duplicates and, if none are found, added to the database exactly as presented in the RADIUS attribute.

Examples

The following example enables this feature:

```
Router (config)# ppp unique address accept-access
```

prc-interval (IPv6)

To configure the hold-down period between partial route calculations (PRCs), use the **prc-interval** command in address family configuration mode. To restore the default interval, use the **no** form of this command.

prc-interval *seconds* [*initial-wait*] [*secondary-wait*]

no prc-interval *seconds*

Syntax Description

seconds	Minimum amount of time between PRCs, in seconds. It can be a number in the range 1 to 120. The default is 5 seconds.
initial-wait	(Optional) Length of time before the first PRC in milliseconds.
secondary-wait	(Optional) Minimum length of time between the first and second PRC in milliseconds.

Command Default

The default is 5 seconds.

Command Modes

Address family configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.6	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The **prc-interval** command is used only in multitopology Intermediate System-to-Intermediate System (IS-IS).

The **prc-interval** command controls how often Cisco IOS software can perform a PRC. Increasing the PRC interval reduces the processor load of the router, but it could slow the convergence.

This command is analogous to the **spf-interval** command, which controls the hold-down period between shortest path first (SPF) calculations.

You can use the **prc-interval** (IPv6) command only when using the IS-IS multitopology for IPv6 feature.

Examples

The following example sets the PRC calculation interval to 20 seconds:

```
Router(config)# router isis
Router(config-router)# address-family ipv6
Router(config-router-af)# prc-interval 20
```

Related Commands

Command	Description
spf-interval (IPv6)	Controls how often Cisco IOS software performs the SPF calculation.

pre-shared-key

To define a preshared key to be used for Internet Key Exchange (IKE) authentication, use the **pre-shared-key** command in keyring configuration mode. To disable the preshared key, use the **no** form of this command.

pre-shared-key {**address** *address* [*mask*] | **hostname** *hostname* | **ipv6** {*ipv6-address* | *ipv6-prefix*}} **key** *key*

no pre-shared-key {**address** *address* [*mask*] | **hostname** *hostname* | **ipv6** {*ipv6-address* | *ipv6-prefix*}} **key** *key*

Syntax Description

address *address* [*mask*]	IP address of the remote peer or a subnet and mask. The *mask* argument is optional.
hostname *hostname*	Fully qualified domain name (FQDN) of the peer.
ipv6	Specifies that an IPv6 address of a remote peer will be used.
ipv6-address	IPv6 address of the remote peer. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
ipv6-prefix	IPv6 prefix of the remote peer.
key *key*	Specifies the secret.

Command Default

None

Command Modes

Keyring configuration (config-keyring)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.3(2)T	This command was modified so that output for the **pre-shared-key** command will show that the preshared key is either encrypted or unencrypted.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.4(4)T	The **ipv6** keyword and the *ipv6-address* and *ipv6-prefix* arguments were added.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

Before configuring preshared keys, you must configure an Internet Security Association and Key Management Protocol (ISAKMP) profile.

Output for the **pre-shared-key** command will show that the preshared key is either unencrypted or encrypted. An output example for an unencrypted preshared key would be as follows:

```
pre-shared-key address 10.1.0.1 key test123
```

An output example for a type 6 encrypted preshared key would be as follows:

```
pre-shared-key address 10.1.0.1 key 6 RHZE[JACMUI\bcbTdELISAAB
```

Examples

The following example shows how to configure a preshared key using an IP address and hostname:

```
Router(config)# crypto keyring vpnkeyring
Router(config-keyring)# pre-shared-key address 10.72.23.11 key vpnkey
Router(config-keyring)# pre-shared-key hostname www.vpn.com key vpnkey
```

Related Commands

Command	Description
crypto keyring	Defines a crypto keyring to be used during IKE authentication.

prefix-delegation

To specify a manually configured numeric prefix to be delegated to a specified client (and optionally a specified identity association for prefix delegation [IAPD] for that client), use the **prefix-delegation** command in DHCP for IPv6 pool configuration mode. To remove the prefix, use the **no** form of this command.

prefix-delegation *ipv6-prefix/prefix-length client-DUID* [**iaid** *iaid*] [*lifetime*]

no prefix-delegation *ipv6-prefix/prefix-length client-DUID* [**iaid** *iaid*]

Syntax Description

ipv6-prefix	(Optional) Specified IPv6 prefix. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/prefix-length	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address).
client-DUID	The DHCP unique identifier (DUID) of the client to which the prefix is delegated.
iaid *iaid*	(Optional) Identity association identifier (IAID), which uniquely identifies an IAPD on the client.
lifetime	(Optional) Sets a length of time over which the requesting router is allowed to use the prefix. The following values can be used: • **valid-lifetime**—The length of time, in seconds, that the prefix remains valid for the requesting router to use. • **at**—Specifies absolute points in time where the prefix is no longer valid and no longer preferred. • **infinite**—Indicates an unlimited lifetime. • **preferred-lifetime**—The length of time, in seconds, that the prefix remains preferred for the requesting router to use. • *valid-month valid-date valid-year valid-time*—A fixed duration of time for hosts to remember router advertisements. The format to be used can be **oct 24 2003 11:45** or **24 oct 2003 11:45**. • *preferred-month preferred-date preferred-year preferred-time*—A fixed duration of time for hosts to remember router advertisements. The format to be used can be **oct 24 2003 11:45** or **24 oct 2003 11:45**.

Command Default

No manually configured prefix delegations exist.

Command Modes

DHCP for IPv6 pool configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

Administrators can manually configure a list of prefixes and associated preferred and valid lifetimes for an IAPD of a specific client that is identified by its DUID. This static binding of client and prefixes can be specified based on users' subscription to an ISP using the **prefix-delegation** *prefix-length* command.

The *client-DUID* argument identifies the client to which the prefix is delegated. All the configured prefixes will be assigned to the specified IAPD of the client. The IAPD to which the prefix is assigned is identified by the **iaid** argument if the **iaid** keyword is configured. If the **iaid** keyword is not configured, the prefix will be assigned to the first IAPD from the client that does not have a static binding. This function is intended to make it convenient for administrators to manually configure prefixes for a client that only sends one IAPD in case it is not easy to know the iaid in advance.

When the delegating router receives a request from a client, it checks whether there is a static binding configured for the IAPD in the client's message. If one is present, the prefixes in the binding are returned to the client. If no such binding is found, the server attempts to assign prefixes for the client from other sources.

Optionally valid and preferred lifetimes can be specified for the prefixes assigned from this pool. Users should coordinate the specified lifetimes with the lifetimes on prefixes from the upstream delegating router if the prefixes were acquired from that router.

The **lifetime** keyword can be specified in one of two ways:

- A fixed duration that stays the same in consecutive advertisements.
- Absolute expiration time in the future so that advertised lifetime decrements in real time, which will result in a lifetime of 0 at the specified time in the future.

The specified length of time is between 60 and 4294967295 seconds or infinity if the **infinite** keyword is specified.

Examples

The following example configures an IAPD for a specified client:

```
prefix-delegation 2001:0DB8::/64 00030001000BBFAA2408
```

Related Commands

Command	Description
ipv6 dhcp pool	Configures a DHCP for IPv6 pool and enters DHCP for IPv6 pool configuration mode.
ipv6 local pool	Configures a local IPv6 prefix pool.
prefix-delegation pool	Specifies a named IPv6 local prefix pool from which prefixes are delegated to DHCP for IPv6 clients.
show ipv6 dhcp pool	Displays DHCP for IPv6 configuration pool information.

prefix-delegation aaa

To specify that prefixes are to be acquired from authorization, authentication, and accounting (AAA) servers, use the **prefix-delegation aaa** command in DHCP for IPv6 pool configuration mode. To disable this feature, use the **no** form of this command.

Cisco IOS Release 12.4(22)T and Earlier Releases and Cisco IOS Release 12.2(18)SXE, Cisco IOS XE Release 2.1, and Later Releases

prefix-delegation aaa [**method-list** *method-list* [**lifetime**] {{*valid-lifetime* | **infinite**} {*valid-lifetime* | **infinite**} | **at** {*date month year time* | *month date year time*} {*date month year time* | *month date year time*}}]

no prefix-delegation aaa method-list *method-list*

Cisco IOS Release 15.0(1)M and Later Releases

prefix-delegation aaa method-list {*method-list* | **default**} [**lifetime** {*valid-lifetime* | **infinite**} {*preferred-lifetime* | **infinite**} | **at** {*date month year time* | *month date year time*} {*date month year time* | *month date year time*}]

no prefix-delegation aaa method-list *method-list*

Syntax Description

method-list	(Optional) Indicates a method list to be defined.
method-list	Configuration type AAA authorization method list that defines how authorization will be performed.
default	Specifies the default method list, nvgened.
lifetime	(Optional) Configures prefix lifetimes.
valid-lifetime	The length of time that the prefix remains valid for the requesting router to use, in seconds. The range is from 60 to 4294967295. The default value is 2592000 seconds.
infinite	Indicates an unlimited lifetime.
preferred-lifetime	The length of time that the prefix remains preferred for the requesting router to use, in seconds. The range is from 60 to 4294967295. The default value is 604800 seconds.
at	Specifies absolute points in time where the prefix is no longer valid and no longer preferred.
date	The date for the valid lifetime to expire.
month	The month for the valid lifetime to expire.
year	The year for the valid lifetime to expire. The range is from 2003 to 2035.
time	The year for the valid lifetime to expire.

Command Default

The default time that the prefix remains valid is 2592000 seconds, and the default time that the prefix remains preferred for the requesting router to use is 604800 seconds.

Command Modes DHCP for IPv6 pool configuration (config-dhcpv6)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.0(1)M	This command was modified. The **default** keyword was added and the command syntax was modified to show that **lifetime** can be configured only to a **method-list**.
Cisco IOS XE Release 2.5	This command was updated. It was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines In order for the Dynamic Host Configuration Protocol (DHCP) for IPv6 server to obtain prefixes from RADIUS servers, you must also configure the AAA client and Point-to-Point Protocol (PPP) on the router. For information on how to configure the AAA client and PPP, see the "Implementing ADSL and Deploying Dial Access for IPv6" module.

Use the **aaa authorization configuration default**, **aaa group server radius**, and **radius-server host** commands to specify a named list of authorization method and RADIUS servers to contact to acquire prefixes, and then apply that named list to the **prefix-delegation aaa** command.

Valid and preferred lifetimes can be specified for the prefixes assigned from AAA servers.

The **prefix-delegation aaa** and **prefix-delegation pool** commands are mutually exclusive in a pool.

Examples The following example shows how to specify the use of a method list named list1:

```
Router> enable
Router# configure terminal
Router(config)# ipv6 dhcp pool name
Router(config-dhcpv6)# prefix-delegation aaa method-list list1
```

Related Commands

Command	Description
aaa authorization configuration default	Downloads static route configuration information from the AAA server using TACACS+ or RADIUS.
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
prefix-delegation pool	Specifies a named IPv6 local prefix pool from which prefixes are delegated to DHCP for IPv6 clients.
radius-server host	Specifies a RADIUS server host.
sip address	Configures a SIP server IPv6 address to be returned in the SIP server's IPv6 address list option to clients.
sip domain-name	Configures an SIP server domain name to be returned in the SIP server's domain name list option to clients.

prefix-delegation pool

To specify a named IPv6 local prefix pool from which prefixes are delegated to Dynamic Host Configuration Protocol (DHCP) for IPv6 clients, use the **prefix-delegation pool** command in DHCP for IPv6 pool configuration mode. To remove a named IPv6 local prefix pool, use the **no** form of this command.

prefix-delegation pool *poolname* [**lifetime** {*valid-lifetime preferred-lifetime*}]

no prefix-delegation pool *poolname*

Syntax Description

poolname	User-defined name for the local prefix pool. The pool name can be a symbolic string (such as "Engineering") or an integer (such as 0).
lifetime	(Optional) Used to set a length of time for the hosts to remember router advertisements. If the optional **lifetime** keyword is configured, both valid and preferred lifetimes must be configured.
valid-lifetime	The amount of time that the prefix remains valid for the requesting router to use. The following values can be used: • *seconds*—The length of time, in seconds, that the prefix remains valid for the requesting router to use. The range is from 60 through 4294967295. The *preferred-lifetime* value cannot exceed the *valid-lifetime* value. • **at**—Specifies absolute points in time where the prefix is no longer valid and no longer preferred. • **infinite**—Indicates an unlimited lifetime. • *valid-month valid-date valid-year valid-time*—A fixed duration of time for hosts to remember router advertisements. The format to be used can be **oct 24 2003 11:45** or **24 oct 2003 11:45**.
preferred-lifetime	The length of time, in seconds, that the prefix remains preferred for the requesting router to use. The following values can be used: • *seconds*—The length of time, in seconds, that the prefix remains valid for the requesting router to use. The range is from 60 through 4294967295. The *preferred-lifetime* value cannot exceed the *valid-lifetime* value. • **at**—Specifies absolute points in time where the prefix is no longer valid and no longer preferred. • **infinite**—Indicates an unlimited lifetime. • *preferred-month preferred-date preferred-year preferred-time*—A fixed duration of time for hosts to remember router advertisements. The format to be used can be **oct 24 2003 11:45** or **24 oct 2003 11:45**

Command Default

No IPv6 local prefix pool is specified.
Valid lifetime is 2592000 seconds (30 days).
Preferred lifetime is 604800 seconds (7 days).

Command Modes

DHCP for IPv6 pool configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

The **prefix-delegation pool** command specifies a named IPv6 local prefix pool from which prefixes are delegated to clients. Use the **ipv6 local pool** command to configure the named IPv6 prefix pool.

Optionally, valid and preferred lifetimes can be specified for the prefixes assigned from this pool. Users should coordinate the specified lifetimes with the lifetimes on prefixes from the upstream delegating router if the prefixes were acquired from that router.

The **lifetime** keyword can be specified in one of two ways:

- A fixed duration that stays the same in consecutive advertisements.
- Absolute expiration time in the future so that advertised lifetime decrements in real time, which will result in a lifetime of 0 at the specified time in the future.

The specified length of time is from 60 to 4,294,967,295 seconds or infinity if the **infinite** keyword is specified.

The Cisco IOS DHCP for IPv6 server can assign prefixes dynamically from an IPv6 local prefix pool, which is configured using the **ipv6 local pool** command and associated with a DHCP for IPv6 configuration pool using the **prefix-delegation pool** command. When the server receives a prefix request from a client, it attempts to obtain unassigned prefixes, if any, from the pool.

After the client releases the previously assigned prefixes, the server will return the prefixes to the pool for reassignment to other clients.

Examples

The following example specifies that prefix requests should be satisfied from the pool called client-prefix-pool. The prefixes should be delegated with the valid lifetime set to 1800 seconds, and the preferred lifetime is set to 600 seconds:

```
prefix-delegation pool client-prefix-pool lifetime 1800 600
```

Related Commands

Command	Description
ipv6 dhcp pool	Configures a DHCP for IPv6 pool and enters DHCP for IPv6 pool configuration mode.
ipv6 local pool	Configures a local IPv6 prefix pool.
prefix-delegation	Specifies a manually configured numeric prefix that is to be delegated to a particular client's IAPD.
show ipv6 dhcp pool	Displays DHCP for IPv6 configuration pool information.

process-min-time percent

Note Effective with Cisco IOS 15.1(1)T release, the **process-min-time percent** command is not available in Cisco IOS 15.1(1)T and later releases. Improvements in Cisco IOS scheduler have made this command unnecessary.

To specify the minimum percentage of CPU process time OSPF takes before the CPU should yield to a process with a higher priority, use the **process-min-time percent** command in router configuration mode. To disable this function, use the **no** form of this command.

process-min-time percent *percentage*

no process-min-time percent

Syntax Description

percentage	Percentage of CPU process time to be used before trying to release the CPU for other processes. The valid value range is from 1 to 100. The default is 25.

Command Default

The default is 25 percent.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
12.2(18)SXF	This command was introduced on the Supervisor Engine 720 and the Supervisor Engine 320.
12.4(4)T	Support for IPv6 was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.1(1)T	This command was removed.

Usage Guidelines

Note Use this command under the direction of Cisco TAC only.

This command is supported by OSPFv2 and OSPFv3.

Use the **process-min-time percent** command to configure the minimum percentage of the process maximum time. Lowering the minimum percentage of CPU usage that a process can utilize is useful in some circumstances to ensure equitable division of CPU resources among different tasks. Once the percentage has been exceeded, CPU control may be given to a higher priority process.

The process maximum time is set using the **process-max-time** command. Use the **process-min-time percent** command in conjunction with the **process-max-time** command.

Examples

The following example shows how to set the percentage of CPU process time to be used before releasing the CPU:

```
Router# configure terminal
Router(config)# router ospf
Router(config-router)# process-min-time percent 35
```

The following example shows how to return to the default setting in IPv4:

```
Router# configure terminal
Router(config)# router ospf
Router(config-router)# no process-min-time percent
```

Related Commands

Command	Description
process-max-time	Configures the amount of time after which a process should voluntarily yield to another process.

protocol ipv6 (ATM)

To map the IPv6 address of a remote node to the ATM permanent virtual circuit (PVC) used to reach the address, use the **protocol ipv6** command in ATM VC configuration mode. To remove the static map, use the **no** form of this command.

protocol ipv6 *ipv6-address* [[**no**] **broadcast**]

no protocol ipv6 *ipv6-address* [[**no**] **broadcast**]

Syntax Description

ipv6-address	Destination IPv6 (protocol) address that is being mapped to a PVC. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
no broadcast	(Optional) Indicates whether the map entry should be used when IPv6 multicast packets (not broadcast packets) are sent to the interface. Pseudobroadcasting is supported. The [**no**] **broadcast** keywords in the **protocol ipv6** command take precedence over the **broadcast** command configured on the same ATM PVC.

Command Default

No mapping is defined.

Command Modes

ATM VC configuration (for an ATM PVC)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Examples

In the following example, two nodes named Cisco 1 and Cisco 2 are connected by a single PVC. The point-to-point subinterface ATM0.132 is used on both nodes to terminate the PVC; therefore, the mapping between the IPv6 addresses of both nodes and the PVC is implicit (no additional mappings are required).

Cisco 1 Configuration

```
interface ATM0
 no ip address
!
interface ATM0.132 point-to-point
 pvc 1/32
```

```
  encapsulation aal5snap
 !
 ipv6 address 2001:0DB8:2222::72/32
```

Cisco 2 Configuration

```
interface ATM0
 no ip address
!
interface ATM0.132 point-to-point
 pvc 1/32
  encapsulation aal5snap
 !
 ipv6 address 2001:0DB8:2222::45/32
```

In the following example, the same two nodes (Cisco 1 and Cisco 2) from the previous example are connected by the same PVC. In this example, however, the point-to-multipoint interface ATM0 is used on both nodes to terminate the PVC; therefore, explicit mappings are required between the link-local and global IPv6 addresses of interface ATM0 on both nodes and the PVC. Additionally, ATM pseudobroadcasts are enabled on the link-local address of interface ATM0 on both nodes.

Cisco 1 Configuration

```
interface ATM0
 no ip address
 pvc 1/32
  protocol ipv6 2001:0DB8:2222::45
  protocol ipv6 FE80::60:2FA4:8291:2 broadcast
  encapsulation aal5snap
 !
 ipv6 address 2001:0DB8:2222::72/32
```

Cisco 2 Configuration

```
interface ATM0
 no ip address
 pvc 1/32
  protocol ipv6 FE80::60:3E47:AC8:C broadcast
  protocol ipv6 2001:0DB8:2222::72
  encapsulation aal5snap
 !
 ipv6 address 2001:0DB8:2222::45/32
```

Related Commands

Command	Description
show atm map	Displays the list of all configured ATM static maps to remote hosts on an ATM network and on ATM bundle maps.

protocol mode

To configure the Cisco IOS Session Initiation Protocol (SIP) stack, use the **protocol mode** command in SIP user-agent configuration mode. To disable the configuration, use the **no** form of this command.

protocol mode {**ipv4** | **ipv6** | **dual-stack** [**preference** {**ipv4** | **ipv6**}]}

no protocol mode

Syntax Description

ipv4	Specifies the IPv4-only mode.
ipv6	Specifies the IPv6-only mode.
dual-stack	Specifies the dual-stack (that is, IPv4 and IPv6) mode.
preference {**ipv4** | **ipv6**}	(Optional) Specifies the preferred dual-stack mode, which can be either IPv4 (the default preferred dual-stack mode) or IPv6.

Command Default

No protocol mode is configured.
The Cisco IOS SIP stack operates in IPv4 mode when the **no protocol mode** or **protocol mode ipv4** command is configured.

Command Modes

SIP user-agent configuration (config-sip-ua)

Command History

Release	Modification
12.4(22)T	This command was introduced.
15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.

Usage Guidelines

The **protocol mode** command is used to configure the Cisco IOS SIP stack in IPv4-only, IPv6-only, or dual-stack mode. For dual-stack mode, the user can (optionally) configure the preferred family, IPv4 or IPv6.

For a particular mode (for example, IPv6-only), the user can configure any address (for example, both IPv4 and IPv6 addresses) and the system will not hide or restrict any commands on the router. SIP chooses the right address for communication based on the configured mode on a per-call basis.

For example, if the domain name system (DNS) reply has both IPv4 and IPv6 addresses and the configured mode is IPv6-only (or IPv4-only), the system discards all IPv4 (or IPv6) addresses and tries the IPv6 (or IPv4) addresses in the order they were received in the DNS reply. If the configured mode is dual-stack, the system first tries the addresses of the preferred family in the order they were received in the DNS reply. If all of the addresses fail, the system tries addresses of the other family.

Examples

The following example configures dual-stack as the protocol mode:

```
Router(config-sip-ua)# protocol mode dual-stack
```

The following example configures IPv6 only as the protocol mode:

```
Router(config-sip-ua)# protocol mode ipv6
```

The following example configures IPv4 only as the protocol mode:

```
Router(config-sip-ua)# protocol mode ipv4
```

The following example configures no protocol mode:

```
Router(config-sip-ua)# no protocol mode
```

Related Commands

Command	Description
sip ua	Enters SIP user-agent configuration mode.

queue-depth (OSPFv3)

To configure the number of incoming packets that the IPv4 Open Shortest Path First version 3 (OSPFv3) process can keep in its queue, use the **queue-depth** command in OSPFv3 router configuration mode. To set the queue depth to its default value, use the **no** form of the command.

queue-depth {**hello** | **update**} {*queue-size* | **unlimited**}

no queue-depth {**hello** | **update**}

Syntax Description

hello	Specifies the queue depth of the OSPFv3 hello process.
update	Specifies the queue depth of the OSPFv3 router process queue.
queue-size	Maximum number of packets in the queue. The range is 1 to 2147483647.
unlimited	Specifies an infinite queue depth.

Command Default

If you do not set a queue size, the OSPFv3 hello process queue depth is unlimited and the OSPFv3 router process (update) queue depth is 200 packets.

Command Modes

OSPFv3 router configuration mode (config-router)

Command History

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

Usage Guidelines

All incoming OSPFv3 packets are initially enqueued in the hello queue. OSPFv3 hello packets are processed directly from this queue, while all other OSPFv3 packet types are subsequently enqueued in the update queue.

If you configure a router with many neighbors and a large database, use the **queue-depth** command to adjust the size of the hello and router queues. Otherwise, packets might be dropped because of queue limits, and OSPFv3 adjacencies may be lost.

Examples

The following example shows how to configure the OSPFv3 update queue to 1500 packets:

```
Router(config)# router ospfv3 1
Router(config-router)# queue-depth update 1500
```

Related Commands

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

radius-server attribute list

To define an accept or reject list name, use the **radius-server attribute list** command in global configuration mode. To remove an accept or reject list name from your configuration, use the **no** form of this command.

radius-server attribute list *list-name*

no radius-server attribute list *list-name*

Syntax Description

list-name	Name for an accept or reject list.

Command Default

List names are not defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(1)DX	This command was introduced.
12.2(2)DD	This command was integrated into Cisco IOS Release 12.2(2)DD.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(13)T	Platform support was added for the Cisco 7401 ASR router.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.3S.	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

A user may configure an accept or reject list with a selection of attributes on the network access server (NAS) for authorization or accounting so unwanted attributes are not accepted and processed. The **radius-server attribute list** command allows users to specify a name for an accept or reject list. This command is used in conjunction with the **attribute** (server-group configuration) command, which adds attributes to an accept or reject list.

Note The list name must be the same as the list name defined in the **accounting** or **authorization** configuration command.

Examples

The following example shows how to configure the reject list "bad-list" for RADIUS authorization and accept list "usage-only" for RADIUS accounting:

```
Router(config)# aaa new-model
Router(config)# aaa authentication ppp default group radius-sg
Router(config)# aaa authorization network default group radius-sg
Router(config)# aaa group server radius radius-sg
Router(config-sg-radius)# server 10.1.1.1
Router(config-sg-radius)# authorization reject bad-list
Router(config-sg-radius)# accounting accept usage-only
Router(config-sg-radius)# exit
Router(config)# radius-server host 10.1.1.1 key mykey1
Router(config)# radius-server attribute list usage-only
Router(config-radius-attrl)# attribute 1,40,42-43,46
Router(config-radius-attrl)# exit
Router(config)# radius-server attribute list bad-list
Router(config-radius-attrl)# attribute 22,27-28,56-59
```

Note Although you cannot configure more than one access or reject list per server group for authorization or accounting, you can configure one list for authorization and one list for accounting per server group.

Related Commands

Command	Description
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
accounting (server-group configuration)	Specifies an accept or reject list for attributes that are to be sent to the RADIUS server in an accounting request.
attribute (server-group configuration)	Adds attributes to an accept or reject list.
authorization (server-group configuration)	Specifies an accept or reject list for attributes that are returned in an Access-Accept packet from the RADIUS server.
radius-server host	Specifies a RADIUS server host.

radius-server host

To specify a RADIUS server host, use the **radius-server host** command in global configuration mode. To delete the specified RADIUS host, use the **no** form of this command.

Cisco IOS Releases 12.2SB and 12.2SR

radius-server host {*hostname* | *ip-address*} [**test username** *user-name*] [**auth-port** *port-number*] [**ignore-auth-port**] [**acct-port** *port-number*] [**ignore-acct-port**] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] [**alias** {*hostname* | *ip-address*}] [**idle-time** *minutes*] [**backoff exponential** {**backoff-retry** *number-of-retransmits* | **max-delay** *minutes*}] [**key** *encryption-key*]

no radius-server host {*hostname* | *ip-address*}

All Other Releases

radius-server host {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] [**alias** {*hostname* | *ip-address*}] [**backoff exponential** {**backoff-retry** *number-of-retransmits* | **max-delay** *minutes*}] [**pac** [**key** *encryption-key*] | **key** *encryption-key*]

no radius-server host {*hostname* | *ip-address*}

Syntax Description

hostname	Domain Name System (DNS) name of the RADIUS server host.
ip-address	IP address of the RADIUS server host.
test username	(Optional) Turns on the automated testing feature for RADIUS server load balancing.
user-name	(Optional) Test user ID username.
auth-port	(Optional) Specifies the User Datagram Protocol (UDP) destination port for authentication requests.
port-number	(Optional) The port number for authentication requests; the host is not used for authentication if the port number is set to 0. If the port number is not specified, the port number defaults to 1645.
ignore-auth-port	(Optional) Turns off the automated testing feature for RADIUS server load balancing on the authentication port.
acct-port	(Optional) Specifies the UDP destination port for accounting requests.
ignore-acct-port	(Optional) Turns off the automated testing feature for RADIUS server load balancing on the accounting port.
timeout *seconds*	(Optional) Specifies the time interval (in seconds) that the router waits for the RADIUS server to reply before retransmitting. This setting overrides the global value of the **radius-server timeout** command. If no timeout value is specified, the global value is used. Enter a value in the range 1 to 1000.
retransmit *retries*	(Optional) Specifies the number of times a RADIUS request is re-sent to a server, if that server is not responding or is responding slowly. This setting overrides the global setting of the **radius-server retransmit** command. If no retransmit value is specified, the global value is used. Enter a value in the range 1 to 100.

key	(Optional) Specifies the authentication and encryption key used between the router and the RADIUS daemon running on this RADIUS server. This key overrides the global setting of the **radius-server key** command. If no key string is specified, the global value is used. The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the **radius-server host** command syntax. This is because the leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in the key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.
string	(Optional) Authentication and encryption key for all RADIUS communications between the router and the RADIUS server. This key must match the encryption used on the RADIUS daemon. All leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.
alias	(Optional) Allows up to eight aliases per line for any given RADIUS server.
idle-time *minutes*	(Optional) Specifies the length of time the server remains idle before it is quarantined and test packets are sent out. • Default is 60 minutes (1 hour). • The valid range is 1 to 35791 seconds.
backoff exponential	(Optional) Specifies the exponential retransmits backup mode.
backoff-retry *number-of-retransmits*	Specifies the exponential backoff retry. • *number-of-retransmits*—Number of backoff retries. Value = 1 through 50. The default is 8.
max-delay *minutes*	Specifies the maximum delay between retransmits. • *minutes*—Value = 1 through 120 minutes. The default is 3 minutes.
pac	(Optional) Specifies that automatic Protected Access Credential (PAC) provisioning is triggered. **Note** The **pac** keyword is mutually exclusive with the shared secret **key** keyword that already exists.
key *encryption-key*	Specifies the per-server encryption key (overrides the default). • *encryption-key*—Can be **0** (specifies that an unencrypted keys follows), **7** (specifies that a hidden key follows), or a line specifying the unencrypted (clear-text) server key.

Defaults

No RADIUS host is specified; use global **radius-server** command values.

RADIUS server load balancing automated testing is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.1	This command was introduced.
12.0(5)T	This command was modified to add options for configuring timeout, retransmission, and key values per RADIUS server.
12.1(3)T	The **alias** keyword was added on the Cisco AS5300 and AS5800 universal access servers.
12.2(15)B	The **backoff exponential**, **backoff-retry**, **key**, and **max-delay** keywords and *number-of-retransmits, encryption-key*, and *minutes* arguments were added.
12.2(28)SB	The **test username** *user-name*, **ignore-auth-port**, **ignore-acct-port**, and **idle-time** *seconds* keywords and arguments were added for configuring RADIUS server load balancing automated testing functionality. **Note** The keywords and arguments added in Cisco IOS Release 12.2(28)SB apply to any subsequent 12.2SB releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA. The keywords and arguments that were added in Cisco IOS Release 12.2(28)SB apply to Cisco IOS Release 12.2(33)SRA and subsequent 12.2SR releases.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T. **Note** The keywords and arguments that were added in Cisco IOS Release 12.2(28)SB do not apply to Cisco IOS Release 12.4(11)T or to subsequent 12.4T releases.
12.2 SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. **Note** The keywords and arguments that were added in Cisco IOS Release 12.2(28)SB do not apply to Cisco IOS Release 12.2SX.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

You can use multiple **radius-server host** commands to specify multiple hosts. The software searches for hosts in the order in which you specify them.

You can specify the keywords of the **radius-server host** command in any order. However, the **pac** keyword always precedes the **key** *encryption-key* keyword.

If you do not specify the port number for authentication requests for both the **acct-port** and the **auth-port** keywords, the port number defaults to 1645.

If no host-specific timeout, retransmit, or key values are specified, the global values apply to each host.

We recommend the use of a test user who is not defined on the RADIUS server for the automated testing of the RADIUS server. This is to protect against security issues that can arise if the test user is not configured correctly.

If you configure one RADIUS server with the nonstandard option and another RADIUS server without the nonstandard option, the RADIUS-server host with the nonstandard option does not accept a predefined host. If you configure the same RADIUS server host IP address for a different UDP destination port for accounting requests using the **acct-port** keyword and a UDP destination port for authentication requests using the **auth-port** keyword with and without the nonstandard option, the RADIUS server does not accept the nonstandard option.

Because entering a line resets all the port numbers, you must specify a host and configure accounting and authentication ports on a single line.

To use separate servers for accounting and authentication, use the zero port value as appropriate.

RADIUS Server Automated Testing (for Cisco IOS Release 12.2(28)SB)

When you use the **radius-server host** command to enable automated testing for RADIUS server load balancing:

- The authentication port is enabled by default. If the port number is not specified, the default port of 1645 is used. To disable the authentication port, specify the **ignore-auth-port** keyword.
- The accounting port is enabled by default. If the port number is not specified, the default port of 1645 is used. To disable the accounting port, specify the **ignore-acct-port** keyword.

Examples

Releases Other than Cisco IOS Release 12.2(28)SB

The following example specifies *host1* as the RADIUS server and uses default ports for both accounting and authentication:

```
radius-server host host1
```

The following example specifies port 1612 as the destination port for authentication requests and port 1616 as the destination port for accounting requests on the RADIUS host named host1:

```
radius-server host host1 auth-port 1612 acct-port 1616
```

Because entering a line resets all the port numbers, you must specify a host and configure accounting and authentication ports on a single line.

The following example specifies the host with IP address 192.0.2.46 as the RADIUS server, uses ports 1612 and 1616 as the authorization and accounting ports, sets the timeout value to 6, sets the retransmit value to 5, and sets “rad123” as the encryption key, matching the key on the RADIUS server:

```
radius-server host 192.0.2.46 auth-port 1612 acct-port 1616 timeout 6 retransmit 5 key
rad123
```

To use separate servers for accounting and authentication, use the zero port value as appropriate.

The following example specifies that RADIUS server host1 be used for accounting but not for authentication, and that RADIUS server host2 be used for authentication but not for accounting:

```
radius-server host host1.example.com auth-port 0
radius-server host host2.example.com acct-port 0
```

The following example specifies four aliases on the RADIUS server with IP address 192.0.2.1:

```
radius-server host 192.0.2.1 auth-port 1646 acct-port 1645
radius-server host 192.0.2.1 alias 192.0.2.2 192.0.2.3 192.0.2.4
```

The following example shows how to enable exponential backoff retransmits on a per-server basis. In this example, assume that the retransmit is configured for three retries and the timeout is configured for 5 seconds; that is, the RADIUS request will be transmitted three times with a delay of 5 seconds. Thereafter, the router will continue to retransmit RADIUS requests with a delayed interval that doubles each time until 32 retries have been achieved. The router will stop doubling the retransmit intervals after the interval surpasses the configured 60 minutes; it will transmit every 60 minutes.

The **pac** keyword allows the PAC-Opaque, which is a variable length field, to be sent to the server during the Transport Layer Security (TLS) tunnel establishment phase. The PAC-Opaque can be interpreted only by the server to recover the required information for the server to validate the peer's identity and authentication. For example, the PAC-Opaque may include the PAC-Key and the PAC's peer identity. The PAC-Opaque format and contents are specific to the issuing PAC server.

The following example configures automatic PAC provisioning on a router. In seed devices, also known as core switches, the PAC-Opaque has to be provisioned so that all RADIUS exchanges can use this PAC-Opaque to enable automatic PAC provisioning for the server being used. All nonseed devices obtain the PAC-Opaque during the authentication phase of a link initialization.

```
enable
configure terminal
radius-server host 10.0.0.1 auth-port 1812 acct-port 1813 pac
```

Cisco IOS Release 12.2(28)SB

The following example shows how to enable RADIUS server automated testing for load balancing with the authorization and accounting ports specified:

```
radius-server host 192.0.2.176 test username test1 auth-port 1645 acct-port 1646
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.
aaa authentication ppp	Specifies one or more AAA authentication method for use on serial interfaces running PPP.
aaa authorization	Sets parameters that restrict network access to a user.
debug aaa test	Shows when the idle timer or dead timer has expired for RADIUS server load balancing.
load-balance	Enables RADIUS server load balancing for named RADIUS server groups.
ppp	Starts an asynchronous connection using PPP.
ppp authentication	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.
radius-server key	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.
radius-server load-balance	Enables RADIUS server load balancing for the global RADIUS server group.
radius-server retransmit	Specifies how many times the Cisco IOS software searches the list of RADIUS server hosts before giving up.
radius-server timeout	Sets the interval a router waits for a server host to reply.
test aaa group	Tests RADIUS load balancing server response manually.
username	Establishes a username-based authentication system, such as PPP CHAP and PAP.

radius-server key

To set the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon, use the **radius-server key** command in global configuration mode. To disable the key, use the **no** form of this command.

radius-server key {***0*** *string* | ***7*** *string*} *string*

no radius-server key

Syntax Description

0	Specifies that an unencrypted key will follow.
string	The unencrypted (cleartext) shared key.
7	Specifies that a hidden key will follow.
string	The hidden shared key.
string	The unencrypted (cleartext) shared key.

Command Default

The authentication and encryption key is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.1	This command was introduced.
12.1(3)T	This command was modified. The *string* argument was modified as follows: • **0** *string* • **7** *string* • *string*
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

After enabling authentication, authorization, and accounting (AAA) authentication with the **aaa new-model** command, you must set the authentication and encryption key using the **radius-server key** command.

Note Specify a RADIUS key after you issue the **aaa new-model** command.

The key entered must match the key used on the RADIUS daemon. All leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.

Examples

The following example sets the authentication and encryption key to "key1":

```
Router(config)# radius-server key key1
```

The following example sets the authentication and encryption key to "anykey." The 7 specifies that a hidden key will follow.

```
service password-encryption
radius-server key 7 anykey
```

After you save your configuration and use the **show-running config** command, an encrypted key will be displayed as follows:

```
Router# show running-config
!
!
 radius-server key 7 19283103834782sda
! The leading 7 indicates that the following text is encrypted.
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
aaa authorization	Sets parameters that restrict user access to a network.
aaa new-model	Enables AAA access control model.
ppp	Starts an asynchronous connection using PPP.
ppp authentication	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.
radius-server host	Specifies a RADIUS server host.
service password-encryption	Encrypt passwords.
username	Establishes a username-based authentication system, such as PPP CHAP and PAP.

radius-server retransmit

To specify the number of times the Cisco IOS software searches the list of RADIUS server hosts before giving up, use the **radius-server retransmit** command in global configuration mode. To disable retransmission, use the **no** form of this command.

radius-server retransmit *retries*

no radius-server retransmit

Syntax Description

retries	Maximum number of retransmission attempts. The range is 0 to 100.

Command Default

The default number of retransmission attempts is 3.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.1	This command was introduced.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

The Cisco IOS software tries all servers, allowing each one to time out before increasing the retransmit count.

If the RADIUS server is only a few hops from the router, we recommend that you configure the RADIUS server retransmit rate to 5.

Examples

The following example shows how to specify a retransmit counter value of five times:

```
Router(config)# radius-server retransmit 5
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
radius-server host	Specifies a RADIUS server host.
radius-server key	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.

Command	Description
radius-server timeout	Sets the interval for which a router waits for a server host to reply.
show radius statistics	Displays the RADIUS statistics for accounting and authentication packets.

radius-server vsa send

To configure the network access server (NAS) to recognize and use vendor-specific attributes (VSAs), use the **radius-server vsa send** command in global configuration mode. To restore the default, use the **no** form of this command.

radius-server vsa send [**accounting** | **authentication** | **cisco-nas-port**] [**3gpp2**]

no radius-server vsa send [**accounting** | **authentication** | **cisco-nas-port**] [**3gpp2**]

Syntax Description

accounting	(Optional) Limits the set of recognized VSAs to only accounting attributes.
authentication	(Optional) Limits the set of recognized VSAs to only authentication attributes.
cisco-nas-port	(Optional) Due to the Internet Engineering Task Force (IETF) requirement for including NAS port information in attribute 87 (Attr87), the Cisco NAS port is obsoleted by default. However, if your servers require this information, then the **cisco-nas-port** keyword can be used to return the Cisco NAS port VSA.
3gpp2	(Optional) Adds Third Generation Partnership Project 2 (3gpp2) Cisco VSAs to this packet type.

Command Default

NAS is not configured to recognize and use VSAs.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3T	This command was introduced.
12.2(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA. The **cisco-nas-port** and **3gpp2** keywords were added to provide backward compatibility for Cisco VSAs.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.3S.	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

The IETF draft standard specifies a method for communicating vendor-specific information between the NAS and the RADIUS server by using the VSA (attribute 26). VSAs allow vendors to support their own extended attributes not suitable for general use. The **radius-server vsa send** command enables the NAS to recognize and use both accounting and authentication VSAs. Use the **accounting** keyword with the **radius-server vsa send** command to limit the set of recognized VSAs to accounting attributes only. Use the **authentication** keyword with the **radius-server vsa send** command to limit the set of recognized VSAs to authentication attributes only.

The Cisco RADIUS implementation supports one vendor-specific option using the format recommended in the specification. The Cisco vendor ID is 9, and the supported option has vendor-type 1, which is named "cisco-avpair." The value is a string with the following format:

```
protocol : attribute sep value *
```

In the preceding example, "protocol" is a value of the Cisco "protocol" attribute for a particular type of authorization; "attribute" and "value" are an appropriate attribute-value (AV) pair defined in the Cisco TACACS+ specification; and "sep" is "=" for mandatory attributes and "*" for optional attributes. This solution allows the full set of features available for TACACS+ authorization to also be used for RADIUS.

For example, the following AV pair causes the Cisco "multiple named ip address pools" feature to be activated during IP authorization (during the PPP Internet Protocol Control Protocol (IPCP) address assignment):

```
cisco-avpair= "ip:addr-pool=first"
```

The following example causes a "NAS Prompt" user to have immediate access to EXEC commands.

```
cisco-avpair= "shell:priv-lvl=15"
```

Other vendors have their own unique vendor IDs, options, and associated VSAs. For more information about vendor IDs and VSAs, see RFC 2138, *Remote Authentication Dial-In User Service (RADIUS)*.

Examples

The following example shows how to configure the NAS to recognize and use vendor-specific accounting attributes:

```
Router(config)# radius-server vsa send accounting
```

Related Commands

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

rd

To specify a route distinguisher (RD) for a VPN routing and forwarding (VRF) instance, use the **rd** command in VRF configuration mode. To remove a route distinguisher, use the **no** form of this command.

rd *route-distinguisher*

no rd *route-distinguisher*

Syntax Description

route-distinguisher	An 8-byte value to be added to an IPv4 prefix to create a VPN IPv4 prefix.

Command Default

No RD is specified.

Command Modes

VRF configuration (config-vrf)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS 12.0(22)S.
12.2(13)T	This command was integrated into Cisco IOS 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	Support for IPv6 was added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
12.2(54)SG	This command was integrated into Cisco IOS Release 12.2(54)SG.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

An RD creates routing and forwarding tables and specifies the default route distinguisher for a VPN. The RD is added to the beginning of the customer's IPv4 prefixes to change them into globally unique VPN-IPv4 prefixes.

An RD is either:

- ASN-related—Composed of an autonomous system number and an arbitrary number.
- IP-address-related—Composed of an IP address and an arbitrary number.

You can enter an RD in either of these formats:

16-bit autonomous-system-number:*your 32-bit number*
For example, 101:3.

32-bit IP address:*your 16-bit number*
For example, 192.168.122.15:1.

Examples

The following example shows how to configure a default RD for two VRFs. It illustrates the use of both autonomous-system-number-relative and IP-address-relative RDs:

```
Router(config)# ip vrf vrf1
Router(config-vrf)# rd 100:3
Router(config-vrf)# exit
Router(config)# ip vrf vrf2
Router(config-vrf)# rd 10.13.0.12:200
```

The following is an example of a VRF for IPv4 and IPv6 that has common policies defined in the global part of the VRF configuration:

```
vrf definition vrf2
 rd 200:1
 route-target both 200:2
!
 address-family ipv4
 exit-address-family
!
 address-family ipv6
 exit-address-family
 end
```

Related Commands

Command	Description
ip vrf	Configures a VRF routing table.
show ip vrf	Displays the set of defined VRFs and associated interfaces.
vrf definition	Configures a VRF routing table and enters VRF configuration mode.

redistribute (IPv6)

To redistribute IPv6 routes from one routing domain into another routing domain, use the **redistribute** command in address family configuration or router configuration mode. To disable redistribution, use the **no** form of this command.

redistribute *source-protocol* [*process-id*] [**include-connected** {**level-1** | **level-1-2** | **level-2**}] [*as-number*] [**metric** {*metric-value* | **transparent**}] [**metric-type** *type-value*] [**match** {**external** [**1** | **2**] | **internal** | **nssa-external** [**1** | **2**]}] [**tag** *tag-value*] [**route-map** *map-tag*]

no redistribute *source-protocol* [*process-id*] [**include-connected**] {**level-1** | **level-1-2** | **level-2**} [*as-number*] [**metric** {*metric-value* | **transparent**}] [**metric-type** *type-value*] [**match** {**external** [**1** | **2**] | **internal** | **nssa-external** [**1** | **2**]}] [**tag** *tag-value*] [**route-map** *map-tag*]

Syntax Description

source-protocol	Source protocol from which routes are being redistributed. It can be one of the following keywords: **bgp**, **connected**, **eigrp**, **isis**, **ospf**, **rip**, or **static**.
process-id	(Optional) For the **bgp** or **eigrp** keyword, the process ID is a Border Gateway Protocol (BGP) autonomous system number, which is a 16-bit decimal number. For the **isis** keyword, the process ID is an optional value that defines a meaningful name for a routing process. You can specify only one IS-IS process per router. Creating a name for a routing process means that you use names when configuring routing. For the **ospf** keyword, the process ID is the number assigned administratively when the Open Shortest Path First (OSPF) for IPv6 routing process is enabled. For the **rip** keyword, the process ID is an optional value that defines a meaningful name for an IPv6 Routing Information Protocol (RIP) routing process.
include-connected	(Optional) Allows the target protocol to redistribute routes learned by the source protocol and connected prefixes on those interfaces over which the source protocol is running.
level-1	Specifies that, for Intermediate System-to-Intermediate System (IS-IS), Level 1 routes are redistributed into other IP routing protocols independently.
level-1-2	Specifies that, for IS-IS, both Level 1 and Level 2 routes are redistributed into other IP routing protocols.
level-2	Specifies that, for IS-IS, Level 2 routes are redistributed into other IP routing protocols independently.
as-number	(Optional) Autonomous system number for the redistributed route.
metric *metric-value*	(Optional) When redistributing from one OSPF process to another OSPF process on the same router, the metric will be carried through from one process to the other if no metric value is specified. When redistributing other processes to an OSPF process, the default metric is 20 when no metric value is specified.
metric transparent	(Optional) Causes RIP to use the routing table metric for redistributed routes as the RIP metric.

metric-type *type-value*	(Optional) For OSPF, specifies the external link type associated with the default route advertised into the OSPF routing domain. It can be one of two values: • **1**—Type 1 external route • **2**—Type 2 external route If no value is specified for the **metric-type** keyword, the Cisco IOS software adopts a Type 2 external route. For IS-IS, the link type can be one of two values: • **internal**—IS-IS metric that is < 63. • **external**—IS-IS metric that is > 64 < 128. The default is **internal**.
match {**external [1 | 2] | internal | nssa-external [1 | 2]**}	(Optional) For OSPF, routes are redistributed into other routing domains using the **match** keyword. It is used with one of the following: • **external [1 | 2]**—Routes that are external to the autonomous system, but are imported into OSPF as Type 1 or Type 2 external routes. • **internal**—Routes that are internal to a specific autonomous system. • **nssa-external** [**1 | 2**]—Routes that are external to the autonomous system but are imported into OSPF, in a not so stubby area (NSSA), for IPv6 as Type 1 or Type 2 external routes.
tag *tag-value*	(Optional) Specifies the 32-bit decimal value attached to each external route. This is not used by OSPF itself. It may be used to communicate information between Autonomous System Boundary Routers (ASBRs). If none is specified, then the remote autonomous system number is used for routes from BGP and Exterior Gateway Protocol (EGP); for other protocols, zero (0) is used.
route-map	(Optional) Specifies the route map that should be checked to filter the importation of routes from this source routing protocol to the current routing protocol. If the **route-map** keyword is not specified, all routes are redistributed. If this keyword is specified, but no route map tags are listed, no routes will be imported.
map-tag	(Optional) Identifier of a configured route map.

Command Default

Route redistribution is disabled.

Command Modes

Address family configuration
Router configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.4(6)T	Support for Enhanced Internal Gateway Routing Protocol (EIGRP) IPv6 was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

Changing or disabling any keyword will not affect the state of other keywords.

A router receiving an IPv6 IS-IS route with an internal metric will consider the cost of the route from itself to the redistributing router plus the advertised cost to reach the destination. An external metric considers only the advertised metric to reach the destination.

IS-IS will ignore any configured redistribution of routes configured with the **include-connected** keyword. IS-IS will advertise a prefix on an interface if either IS-IS is running over the interface or the interface is configured as passive.

Routes learned from IPv6 routing protocols can be redistributed into IPv6 IS-IS at Level 1 into an attached area or at Level 2. The **level-1-2** keyword allows both Level 1 and Level 2 routes in a single command.

For IPv6 RIP, use the **redistribute** command to advertise static routes as if they were directly connected routes.

Caution Advertising static routes as directly connected routes can cause routing loops if improperly configured.

Redistributed IPv6 RIP routing information should always be filtered by the **distribute-list prefix-list** router configuration command. Use of the **distribute-list prefix-list** command ensures that only those routes intended by the administrator are passed along to the receiving routing protocol.

Note The **metric** value specified in the **redistribute** command for IPv6 RIP supersedes the **metric** value specified using the **default-metric** command.

Note In IPv4, if you redistribute a protocol, by default you also redistribute the subnet on the interfaces over which the protocol is running. In IPv6 this is not the default behavior. To redistribute the subnet on the interfaces over which the protocol is running in IPv6, use the **include-connected** keyword. In IPv6 this functionality is not supported when the source protocol is BGP.

When the **no redistribute** command is configured, the parameter settings are ignored when the client protocol is IS-IS or EIGRP.

IS-IS redistribution will be removed completely when IS-IS level 1 and level 2 are removed by the user. IS-IS level settings can be configured using the **redistribute** command only.

The default redistribute type will be restored to OSPF when all route type values are removed by the user.

Examples

The following example configures IPv6 IS-IS to redistribute IPv6 BGP routes. The metric is specified as 5, and the metric type will be set to external, indicating that it has lower priority than internal metrics.

```
Router(config)# router isis
Router(config-router)# address-family ipv6
Router(config-router-af)# redistribute bgp 64500 metric 5 metric-type external
```

The following example redistributes IPv6 BGP routes into the IPv6 RIP routing process named cisco:

```
Router(config)# ipv6 router rip cisco
Router(config-router)# redistribute bgp 42
```

The following example redistributes IS-IS for IPv6 routes into the OSPF for IPv6 routing process 1:

```
Router(config)# ipv6 router ospf 1
Router(config-router)# redistribute isis 1 metric 32 metric-type 1 tag 85
```

In the following example, ospf 1 redistributes the prefixes 2001:1:1::/64 and 2001:99:1::/64 and any prefixes learned through rip 1:

```
interface ethernet0/0
 ipv6 address 2001:1:1::90/64
 ipv6 rip 1 enable

interface ethernet1/1
 ipv6 address 2001:99:1::90/64
 ipv6 rip 1 enable

interface ethernet2/0
 ipv6 address 2001:1:2::90/64
 ipv6 ospf 1 area 1

ipv6 router ospf 1
  redistribute rip 1 include-connected
```

The following configuration example and output show the **no redistribute** command parameters when the last route type value is removed:

```
Router(config-router)# redistribute rip process1 metric 7
Router(config-router)# do show run | include redistribute
 redistribute rip process1 metric 7
Router(config-router)# no redistribute rip process1 metric 7
Router(config-router)# do show run | include redistribute
 redistribute rip process1
Router(config-router)#
```

Related Commands

Command	Description
default-metric	Specifies a default metric for redistributed routes.
distribute-list prefix-list (IPv6 EIGRP)	Applies a prefix list to EIGRP for IPv6 routing updates that are received or sent on an interface.
distribute-list prefix-list (IPv6 RIP)	Applies a prefix list to IPv6 RIP routing updates that are received or sent on an interface.
redistribute isis (IPv6)	Redistributes IPv6 routes from one routing domain into another routing domain using IS-IS as both the target and source protocol.

redistribute (OSPFv3)

To redistribute IPv6 and IPv4 routes from one routing domain into another routing domain, use the **redistribute** command in IPv6 or IPv4 address family configuration mode. To disable redistribution, use the **no** form of this command.

redistribute *source-protocol* [*process-id*] [*options*]

no redistribute *source-protocol* [*process-id*] [*options*]

Syntax Description

source-protocol	Source protocol from which routes are being redistributed. It can be one of the following keywords: **bgp**, **connected**, **eigrp**, **isis**, **nd**, **nemo**, **ospfv3**, **ospf**, **rip**, or **static**.
process-id	(Optional) For the **bgp** or **eigrp** keyword, the process ID is a Border Gateway Protocol (BGP) autonomous system number, which is a 16-bit decimal number. For the **isis** keyword, the process ID is an optional value that defines a meaningful name for a routing process. You can specify only one IS-IS process per router. Creating a name for a routing process means that you use names when configuring routing. For the **ospfv3** keyword, the process ID is the number assigned administratively when the Open Shortest Path First version 3 (OSPFv3) routing process is enabled. For the **rip** keyword, the process ID is an optional value that defines a meaningful name for an IPv6 Routing Information Protocol (RIP) routing process.
options	(Optional)

Command Default

Default redistribute type is OSPFv3.

Command Modes

IPv6 address family configuration (config-router-af)
IPv4 address family configuration (config-router-af)

Command History

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

Usage Guidelines

Changing or disabling any keyword will not affect the state of other keywords.

For the IPv6 address family (AF), the **ospf** option refers to an OSPFv3 process. For the IPv4 address family, the **ospfv3** option specifies an OSPFv3 process, and the **ospf** option refers to an OSPFv2 process.

A router receiving an IPv6 IS-IS route with an internal metric will consider the cost of the route from itself to the redistributing router plus the advertised cost to reach the destination. An external metric considers only the advertised metric to reach the destination.

IS-IS will ignore any configured redistribution of routes configured with the **include-connected** keyword. IS-IS will advertise a prefix on an interface if either IS-IS is running over the interface or the interface is configured as passive.

Routes learned from IPv6 routing protocols can be redistributed into IPv6 IS-IS at Level 1 into an attached area or at Level 2. The **level-1-2** keyword allows both Level 1 and Level 2 routes in a single command.

For IPv6 RIP, use the **redistribute** command to advertise static routes as if they were directly connected routes.

Caution Advertising static routes as directly connected routes can cause routing loops if improperly configured.

Redistributed IPv6 RIP routing information should always be filtered by the **distribute-list prefix-list** router configuration command. Use of the **distribute-list prefix-list** command ensures that only those routes intended by the administrator are passed along to the receiving routing protocol.

Note The **metric** value specified in the **redistribute** command for IPv6 RIP supersedes the **metric** value specified using the **default-metric** command.

Note In IPv4, if you redistribute a protocol, by default you also redistribute the subnet on the interfaces over which the protocol is running. In IPv6, this is not the default behavior. To redistribute the subnet on the interfaces over which the protocol is running in IPv6, use the **include-connected** keyword. In IPv6, this functionality is not supported when the source protocol is BGP.

When the **no redistribute** command is configured, the parameter settings are ignored when the client protocol is IS-IS or EIGRP.

IS-IS redistribution will be removed completely when IS-IS level 1 and level 2 are removed by the user. IS-IS level settings can be configured using the **redistribute** command only.

The default redistribute type will be restored to OSPFv3 when all route type values are removed by the user.

Examples

The following example :

Related Commands

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

redistribute isis (IPv6)

To redistribute IPv6 routes from one routing domain into another routing domain using Intermediate System-to-Intermediate System (IS-IS) as both the target and source protocol, use the **redistribute isis** command in address family configuration. To disable redistribution, use the **no** form of this command.

redistribute isis [*process-id*] {**level-1** | **level-2**} **into** {**level-1** | **level-2**} **distribute-list** *list-name*

no redistribute isis [*process-id*] {**level-1** | **level-2**} **into** {**level-1** | **level-2**} **distribute-list** *list-name*

Syntax Description

process-id	(Optional) An optional *tag* value that defines a meaningful name for a routing process. You can specify only one IS-IS process per router. Creating a name for a routing process means that you use names when configuring routing.
level-1	Specifies that IS-IS Level 1 routes are redistributed into other IP routing protocols independently.
level-2	Specifies that IS-IS Level 2 routes are redistributed into other IP routing protocols independently.
into	Distributes IS-IS Level 1 or Level 2 routes into Level 1 or Level 2 in another IS-IS instance.
distribute-list	Distribute list used for the redistributed route.
list-name	Name of the distribute list for the redistributed route.

Command Default

Route redistribution is disabled.
process-id: No process ID is defined.

Command Modes

Address family configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
Cisco IOS XE Release 2.4	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

Changing or disabling any keyword will not affect the state of other keywords.

A router receiving an IPv6 IS-IS route with an internal metric will consider the cost of the route from itself to the redistributing router plus the advertised cost to reach the destination. An external metric only considers the advertised metric to reach the destination.

IS-IS will ignore any configured redistribution of routes configured with the **connected** keyword. IS-IS will advertise a prefix on an interface if either IS-IS is running over the interface or the interface is configured as passive.

Routes learned from IPv6 routing protocols can be redistributed into IPv6 IS-IS at Level 1 into an attached area or at Level 2. The **level-1-2** keyword allows both Level 1 and Level 2 routes in a single command.

Examples

The following examples shows how to redistribute IPv6 routes from level 1 to level 2:

```
redistribute isis level-1 into level-2
```

Related Commands

Command	Description
default-metric	Specifies a default metric for redistributed routes.
redistribute (IPv6)	Redistributes IPv6 routes from one routing domain into another routing domain.

register (mobile router)

To control the registration parameters of the IPv6 mobile router, use the **register** command in mobile router configuration mode or IPv6 mobile router configuration mode. To return the registration parameters to their default settings, use the **no** form of this command.

register {**extend expire** *seconds* **retry** *number* **interval** *seconds* | **lifetime** *seconds* | **retransmit initial** *milliseconds* **maximum** *milliseconds* **retry** *number*}

no register {**extend expire** *seconds* **retry** *number* **interval** *seconds* | **lifetime** *seconds* | **retransmit initial** *milliseconds* **maximum** *milliseconds* **retry** *number*}

Syntax Description

extend	Reregisters before the lifetime expires.
expire *seconds*	Specifies the time (in seconds) in which to send a registration request before expiration. In IPv4, the range is from 1 to 3600; the default is 120. In IPv6, the range is from 1 to 600.
retry *number*	Specifies the number of times the mobile router retries sending a registration request if no reply is received. In both IPv4 and IPv6, the range is from 0 to 10; the default is 3. A value of 0 means no retry. The mobile router stops sending registration requests after the maximum number of retries is attempted.
interval *seconds*	Specifies the time (in seconds) that the mobile router waits before sending another registration request if no reply is received. In IPv4, the range is from 1 to 3600; the default is 10. In IPv6, the range is from 1 to 60.
lifetime *seconds*	Specifies the requested lifetime (in seconds) of each registration. The shortest value between the configured lifetime and the foreign agent advertised registration lifetime is used. In IPv4, the range is from 3 to 65534; the default is 65534 (infinity). In IPv6, the range is from 4 to 262143; the default is 262143 (infinity). This default ensures that the advertised lifetime is used, excluding infinity.
retransmit initial *milliseconds*	Specifies the wait period (in milliseconds) before sending a retransmission the first time no reply is received from the foreign agent. In IPv4, the range is from 10 to 10000 milliseconds (10 seconds); the default is 1000 milliseconds (1 second). In IPv6, the range is from 1000 to 256000.
maximum *milliseconds* **retry** *number*	Specifies the maximum wait period (in milliseconds) before retransmission of a registration request. In IPv4, the range is 10 to 10000 (10 seconds); the default is 5000 milliseconds (5 seconds). In IPv6, the maximum range is from 1000 to 256000. In IPv6, the retry number range is from 0 to 10. Each successive retransmission timeout period is twice the previous period, if the previous period was less than the maximum value. Retransmission stops after the maximum number of retries.

Command Default

The registration parameters of the IPv6 mobile router are used.

Command Modes

Mobile router configuration
IPv6 mobile router configuration (IPv6-mobile-router)

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.4(20)T	Support for IPv6 was added.

Usage Guidelines

The **register lifetime** *seconds* command configures the lifetime that the mobile router requests in a registration request. The home agent also has lifetimes that are set. If the registration request from a mobile router has a greater lifetime than the registration reply from the home agent, the lifetime set on the home agent will be used for the registration. If the registration request lifetime from the mobile router is less than the registration reply from the home agent, the lifetime set on the mobile router will be used. Thus, the smaller lifetime between the home agent and mobile router is used for registration.

Examples

The following example specifies a registration lifetime of 600 seconds:

```
ip mobile router
 address 10.1.1.10 255.255.255.0
 home-agent 10.1.1.20
 register lifetime 600
```

Related Commands

Command	Description
ipv6 mobile router	Enables IPv6 NEMO functionality on the router and places the router in IPv6 mobile router mode.
show ip mobile router	Displays configuration information and monitoring statistics about the mobile router.
show ip mobile router registration	Displays the pending and accepted registrations of the mobile router.

registrar

To enable Session Initiation Protocol (SIP) gateways to register E.164 numbers on behalf of analog telephone voice ports (FXS), IP phone virtual voice ports (EFXS), and Skinny Client Control Protocol (SCCP) phones with an external SIP proxy or SIP registrar, use the **registrar** command in SIP UA configuration mode. To disable registration of E.164 numbers, use the **no** form of this command.

registrar {**dhcp** | [*registrar-index*] *registrar-server-address* [**:***port*]} [**auth-realm** *realm*] [**expires** *seconds*] [**random-contact**] [**refresh-ratio** *ratio-percentage*] [**scheme** {**sip** | **sips**}] [**tcp**] [*type*] [**secondary**]

no registrar [*registrar-index* | **secondary**]

Syntax Description

dhcp	(Optional) Specifies that the domain name of the primary registrar server is retrieved from a DHCP server (cannot be used to configure secondary or multiple registrars).
registrar-index	(Optional) A specific registrar to be configured, allowing configuration of multiple registrars (maximum of six). Range is 1 to 6.
registrar-server-address	The SIP registrar server address to be used for endpoint registration. This value can be entered in one of three formats: • **dns:***address*—the Domain Name System (DNS) address of the primary SIP registrar server (the **dns:** delimiter must be included as the first four characters). • **ipv4:***address*—the IP address of the SIP registrar server (the **ipv4:** delimiter must be included as the first five characters). • **ipv6:[***address*]—the IPv6 address of the SIP registrar server (the **ipv6:** delimiter must be included as the first five characters and the address itself must include opening and closing square brackets).
[**:***port*]	(Optional) The SIP port number (the colon delimiter is required).
auth-realm	(Optional) Specifies the realm for preloaded authorization.
realm	The realm name.
expires *seconds*	(Optional) Specifies the default registration time, in seconds. Range is 60 to 65535. Default is 3600.
random-contact	(Optional) Specifies the Random String Contact header used to identify the registration session.
refresh-ratio *ratio-percentage*	(Optional) Specifies the registration refresh ratio, in percentage. Range is 1 to 100. Default is 80.
scheme {**sip**	**sips**}	(Optional) Specifies the URL scheme. The options are SIP (**sip**) or secure SIP (**sips**), depending on your software installation**.** The default is **sip**.
tcp	(Optional) Specifies TCP. If not specified, the default is User Datagram Protocol UDP.

type	(Optional) The registration type. **Note** The *type* argument cannot be used with the **dhcp** option.
secondary	(Optional) Specifies a secondary SIP registrar for redundancy if the primary registrar fails. This option is not valid if specifying DHCP or if configuring multiple registrars. **Note** You cannot configure any other optional settings once you enter the **secondary** keyword—specify all other settings first.

Command Default

Registration is disabled.

Command Modes

SIP UA configuration (config-sip-ua)

Command History

Release	Modification
12.2(15)ZJ	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4(6)T	This command was modified. The **tls** keyword and the **scheme** keyword with the *string* argument were added.
12.4(22)T	This command was modified. Support for IPv6 addresses was added.
12.4(22)YB	This command was modified. The **dhcp**, **random-contact and refresh-ratio** keywords were added. Additionally, the **aor-domain** keyword and the **tls** option for the **tcp** keyword were removed.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
15.0(1)XA	This command was modified. The *registrar-index* argument for support of multiple registrars on SIP trunks was added.
15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.
15.1(2)T	This command was modified. The **auth-realm** keyword was added.

Usage Guidelines

Use the **registrar dhcp** or **registrar** *registrar-server-address* command to enable the gateway to register E.164 telephone numbers with primary and secondary external SIP registrars. In Cisco IOS Release 15.0(1)XA and later releases, endpoints on Cisco IOS SIP time-division multiplexing (TDM) gateways, Cisco Unified Border Elements (Cisco UBEs), and Cisco Unified Communications Manager Express (Cisco Unified CME) can be registered to multiple registrars using the **registrar** *registrar-index* command.

By default, Cisco IOS SIP gateways do not generate SIP register messages.

Note When entering an IPv6 address, you must include square brackets around the address value.

Examples

The following example shows how to configure registration with a primary and secondary registrar:

```
Router> enable
Router# configure terminal
```

```
Router(config)# sip-ua
Router(config-sip-ua)# retry invite 3
Router(config-sip-ua)# retry register 3
Router(config-sip-ua)# timers register 150
Router(config-sip-ua)# registrar ipv4:209.165.201.1 expires 14400 secondary
```

The following example shows how to configure a device to register with the SIP server address received from the DHCP server. The **dhcp** keyword is available only for configuration by the primary registrar and cannot be used if configuring multiple registrars.

```
Router> enable
Router# configure terminal
Router(config)# sip-ua
Router(config-sip-ua)# registrar dhcp expires 14400
```

The following example shows how to configure a primary registrar using an IP address with TCP:

```
Router> enable
Router# configure terminal
Router(config)# sip-ua
Router(config-sip-ua)# retry invite 3
Router(config-sip-ua)# retry register 3
Router(config-sip-ua)# timers register 150
Router(config-sip-ua)# registrar ipv4:209.165.201.3 tcp
```

The following example shows how to configure a URL scheme with SIP security:

```
Router> enable
Router# configure terminal
Router(config)# sip-ua
Router(config-sip-ua)# retry invite 3
Router(config-sip-ua)# retry register 3
Router(config-sip-ua)# timers register 150
Router(config-sip-ua)# registrar ipv4:209.165.201.7 scheme sips
```

The following example shows how to configure a secondary registrar using an IPv6 address:

```
Router> enable
Router# configure terminal
Router(config)# sip-ua
Router(config-sip-ua)# registrar ipv6:[3FFE:501:FFFF:5:20F:F7FF:FE0B:2972] expires 14400
secondary
```

The following example shows how to configure all POTS endpoints to two registrars using DNS addresses:

```
Router> enable
Router# configure terminal
Router(config)# sip-ua
Router(config-sip-ua)# registrar 1 dns:example1.com expires 180
Router(config-sip-ua)# registrar 2 dns:example2.com expires 360
```

The following example shows how to configure the realm for preloaded authorization using the registrar server address:

```
Router> enable
Router# configure terminal
Router(config)# sip-ua
Router(config-sip-ua)# registrar 2 192.168.140.3:8080 auth-realm example.com expires 180
```

Related Commands

Command	Description
authentication (dial peer)	Enables SIP digest authentication on an individual dial peer.
authentication (SIP UA)	Enables SIP digest authentication.
credentials (SIP UA)	Configures a Cisco UBE to send a SIP registration message when in the UP state.

Command	Description
localhost	Configures global settings for substituting a DNS localhost name in place of the physical IP address in the From, Call-ID, and Remote-Party-ID headers of outgoing messages.
retry register	Sets the total number of SIP register messages to send.
show sip-ua register status	Displays the status of E.164 numbers that a SIP gateway has registered with an external primary or secondary SIP registrar.
timers register	Sets how long the SIP UA waits before sending register requests.
voice-class sip localhost	Configures settings for substituting a DNS localhost name in place of the physical IP address in the From, Call-ID, and Remote-Party-ID headers of outgoing messages on an individual dial peer, overriding the global setting.

remark (IPv6)

To write a helpful comment (remark) for an entry in an IPv6 access list, use the **remark** command in IPv6 access list configuration mode. To remove the remark, use the **no** form of this command.

remark *text-string*

no remark *text-string*

Syntax Description

text-string	Comment that describes the access list entry, up to 100 characters long.

Command Default

IPv6 access list entries have no remarks.

Command Modes

IPv6 access list configuration

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **remark** (IPv6) command is similar to the **remark** (IP) command, except that it is IPv6-specific.

The remark can be up to 100 characters long; anything longer is truncated.

Examples

The following example configures a remark for the IPv6 access list named TELNETTING. The remark is specific to not letting the Marketing subnet use outbound Telnet.

```
ipv6 access-list TELNETTING
 remark Do not allow Marketing subnet to telnet out
 deny tcp 2001:0DB8:0300:0201::/64 any eq telnet
```

Related Commands

Command	Description
ipv6 access-list	Defines an IPv6 access list and enters IPv6 access list configuration mode.
show ipv6 access-list	Displays the contents of all current IPv6 access lists.

retry register

Usage Guidelines

To set the total number of Session Initiation Protocol (SIP) register messages that the gateway should send, use the **retry register** command in SIP user-agent configuration mode. To reset this number to the default, use the **no** form of this command.

retry register *retries* [**exhausted-random-interval minimum** *minutes* **maximum** *minutes*]

no retry register

Syntax Description

retries	Total number of register messages that the gateway should send. The range is from 1 to 10, and the default is 10 retries.
exhausted-random-interval	Specifies that the register request is generated within the defined range of time intervals.
minimum *minutes*	Specifies the minimum time interval range in minutes that will be used as the interval before the next registration is sent.
maximum *minutes*	Specifies the maximum time interval range in minutes that will be used as the interval before the next registration is sent.

Command Default

The gateway sends ten retries.

Command Modes

SIP UA configuration

Command History

Release	Modification
12.2(15)ZJ	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4(22)T	This command was modified. Support for IPv6 was added.
12.4(22)YB	The **exhausted-random-interval** keyword was added.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

Use the default number of 10 when possible. Lower values such as 1 can lead to an increased chance of the message not being received by the other user agent.

Examples

The following example specifies that the gateway sends nine register messages:

```
sip-ua
 retry register 9
```

The following example specifies that the gateway sends six register message, and that a random number, between the 2 and 5 minutes will be used as the interval before the next registration is sent

```
sip-ua
 retry register 6 exhausted-random-interval minimum 2 maximum 5
```

Related Commands

Command	Description
registrar	Enables SIP gateways to register E.164 numbers on behalf of analog telephone voice ports (FXS), IP phone virtual voice ports (EFXS), and SCCP phones with an external SIP proxy or SIP registrar.
timers register	Sets how long the SIP user agent waits before sending register requests.

revocation-check

To check the revocation status of a certificate, use the **revocation-check** command in ca-trustpoint configuration mode. To disable this functionality, use the **no** form of this command.

revocation-check *method1* [*method2*[*method3*]]

no revocation-check *method1* [*method2*[*method3*]]

Syntax Description

method1 [*method2*[*method3*]]	Method used by the router to check the revocation status of the certificate. Available methods are as follows: • **crl**—Certificate checking is performed by a certificate revocation list (CRL). This is the default behavior. • **none**—Certificate checking is not required. • **ocsp**—Certificate checking is performed by an online certificate status protocol (OCSP) server. If a second and third method are specified, each method will be used only if the previous method returns an error, such as a server being down.

Defaults

After a trustpoint is enabled, the default is set to **revocation-check crl**, which means that CRL checking is mandatory.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.3(2)T	This command was introduced. This command replaced the **crl best-effort** and **crl optional** commands.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(24)T	Support for IPv6 Secure Neighbor Discovery (SeND) was added.

Usage Guidelines

Use the **revocation-check** command to specify at least one method that is to be used to ensure that the certificate of a peer has not been revoked.

If your router does not have the applicable CRL and is unable to obtain one or if the OCSP server returns an error, your router will reject the peer's certificate—unless you include the **none** keyword in your configuration. If the **none** keyword is configured, a revocation check will not be performed and the certificate will always be accepted. If the **revocation-check none** command is configured, you cannot manually download the CRL via the **crypto pki crl request** command because the manually downloaded CRL may not be deleted after it expires. The expired CRL can cause all certificate verifications to be denied.

Note The **none** keyword replaces the **optional** keyword that is available from the **crl** command. If you enter the **crl optional** command, it will be written back as the **revocation-check none** command. However, there is a difference between the **crl optional** command and the **revocation-check none** command. The **crl optional** command will perform revocation checks against any applicable in-memory CRL. If a CRL is not available, a CRL will not be downloaded and the certificate is treated as valid; the **revocation-check none** command ignores the revocation check completely and always treats the certificate as valid.

Also, the **crl** and **none** keywords issued together replace the **best-effort** keyword that is available from the **crl** command. If you enter the **crl best-effort** command, it will be written back as the **revocation-check crl none** command.

Examples

The following example shows how to configure the router to use the OCSP server that is specified in the AIA extension of the certificate:

```
Router(config)# crypto pki trustpoint mytp
Router(ca-trustpoint)# revocation-check ocsp
```

The following example shows how to configure the router to download the CRL from the CDP; if the CRL is unavailable, the OCSP server that is specified in the Authority Info Access (AIA) extension of the certificate will be used. If both options fail, certificate verification will also fail.

```
Router(config)# crypto pki trustpoint mytp
Router(ca-trustpoint)# revocation-check crl ocsp
```

The following example shows how to configure your router to use the OCSP server at the HTTP URL “http://myocspserver:81.” If the server is down, revocation check will be ignored.

```
Router(config)# crypto pki trustpoint mytp
Router(ca-trustpoint)# ocsp url http://myocspserver:81
Router(ca-trustpoint)# revocation-check ocsp none
```

Related Commands

Command	Description
crl query	Queries the CRL to ensure that the certificate of the peer has not been revoked.
crypto pki trustpoint	Declares the CA that your router should use.
ocsp url	Enables an OCSP server.

router bgp

To configure the Border Gateway Protocol (BGP) routing process, use the **router bgp** command in global configuration mode. To remove a BGP routing process, use the **no** form of this command.

router bgp *autonomous-system-number*

no router bgp *autonomous-system-number*

Syntax Description

autonomous-system-number	Number of an autonomous system that identifies the router to other BGP routers and tags the routing information that is passed along. Number in the range from 1 to 65535. • In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, 4-byte autonomous system numbers are supported in the range from 65536 to 4294967295 in asplain notation and in the range from 1.0 to 65535.65535 in asdot notation. • In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, 4-byte autonomous system numbers are supported in the range from 1.0 to 65535.65535 in asdot notation only. For more details about autonomous system number formats, see the "Usage Guidelines" section.

Command Default

No BGP routing process is enabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	This command was modified. Support for IPv6 was added.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX.
12.2(33)SB	This command was modified. Support for IPv6 was added.
12.0(32)S12	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(24)T	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.

Release	Modification
Cisco IOS XE Release 2.3	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SXI1	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
12.2(33)SRE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.

Usage Guidelines

This command allows you to set up a distributed routing core that automatically guarantees the loop-free exchange of routing information between autonomous systems.

Prior to January 2009, BGP autonomous system numbers that were allocated to companies were 2-octet numbers in the range from 1 to 65535 as described in RFC 4271, *A Border Gateway Protocol 4 (BGP-4)*. Due to increased demand for autonomous system numbers, the Internet Assigned Number Authority (IANA) will start in January 2009 to allocate four-octet autonomous system numbers in the range from 65536 to 4294967295. RFC 5396, *Textual Representation of Autonomous System (AS) Numbers*, documents three methods of representing autonomous system numbers. Cisco has implemented the following two methods:

- Asplain—Decimal value notation where both 2-byte and 4-byte autonomous system numbers are represented by their decimal value. For example, 65526 is a 2-byte autonomous system number and 234567 is a 4-byte autonomous system number.
- Asdot—Autonomous system dot notation where 2-byte autonomous system numbers are represented by their decimal value and 4-byte autonomous system numbers are represented by a dot notation. For example, 65526 is a 2-byte autonomous system number and 1.169031 is a 4-byte autonomous system number (this is dot notation for the 234567 decimal number).

For details about the third method of representing autonomous system numbers, see RFC 5396.

Note In Cisco IOS releases that include 4-byte ASN support, command accounting and command authorization that include a 4-byte ASN number are sent in the asplain notation irrespective of the format that is used on the command-line interface.

Asdot Only Autonomous System Number Formatting

In Cisco IOS Release 12.0(32)S12, 12.4(24)T, Cisco IOS XE Release 2.3, and later releases, the 4-octet (4-byte) autonomous system numbers are entered and displayed only in asdot notation, for example, 1.10 or 45000.64000. When using regular expressions to match 4-byte autonomous system numbers the asdot format includes a period which is a special character in regular expressions. A backslash must be entered before the period for example, 1\.14, to ensure the regular expression match does not fail. Table 46 shows

the format in which 2-byte and 4-byte autonomous system numbers are configured, matched in regular expressions, and displayed in **show** command output in Cisco IOS images where only asdot formatting is available.

Table 46 Asdot Only 4-Byte Autonomous System Number Format

Format	Configuration Format	Show Command Output and Regular Expression Match Format
asdot	2-byte: 1 to 65535 4-byte: 1.0 to 65535.65535	2-byte: 1 to 65535 4-byte: 1.0 to 65535.65535

Asplain as Default Autonomous System Number Formatting

In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, the Cisco implementation of 4-byte autonomous system numbers uses asplain as the default display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain and asdot format. In addition, the default format for matching 4-byte autonomous system numbers in regular expressions is asplain, so you must ensure that any regular expressions to match 4-byte autonomous system numbers are written in the asplain format. If you want to change the default **show** command output to display 4-byte autonomous system numbers in the asdot format, use the **bgp asnotation dot** command under router configuration mode. When the asdot format is enabled as the default, any regular expressions to match 4-byte autonomous system numbers must be written using the asdot format, or the regular expression match will fail. Table 47 and Table 48 show that although you can configure 4-byte autonomous system numbers in either asplain or asdot format, only one format is used to display **show** command output and control 4-byte autonomous system number matching for regular expressions, and the default is asplain format. To display 4-byte autonomous system numbers in **show** command output and to control matching for regular expressions in the asdot format, you must configure the **bgp asnotation dot** command. After enabling the **bgp asnotation dot** command, a hard reset must be initiated for all BGP sessions by entering the **clear ip bgp *** command.

Note If you are upgrading to an image that supports 4-byte autonomous system numbers, you can still use 2-byte autonomous system numbers. The **show** command output and regular expression match are not changed and remain in asplain (decimal value) format for 2-byte autonomous system numbers regardless of the format configured for 4-byte autonomous system numbers.

Table 47 Default Asplain 4-Byte Autonomous System Number Format

Format	Configuration Format	Show Command Output and Regular Expression Match Format
asplain	2-byte: 1 to 65535 4-byte: 65536 to 4294967295	2-byte: 1 to 65535 4-byte: 65536 to 4294967295
asdot	2-byte: 1 to 65535 4-byte: 1.0 to 65535.65535	2-byte: 1 to 65535 4-byte: 65536 to 4294967295

Table 48 Asdot 4-Byte Autonomous System Number Format

Format	Configuration Format	Show Command Output and Regular Expression Match Format
asplain	2-byte: 1 to 65535 4-byte: 65536 to 4294967295	2-byte: 1 to 65535 4-byte: 1.0 to 65535.65535
asdot	2-byte: 1 to 65535 4-byte: 1.0 to 65535.65535	2-byte: 1 to 65535 4-byte: 1.0 to 65535.65535

Reserved and Private Autonomous System Numbers

In Cisco IOS Release 12.0(32)S12, 12.0(32)SY8, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, 12.4(24)T, Cisco IOS XE Release 2.3 and later releases, the Cisco implementation of BGP supports RFC 4893. RFC 4893 was developed to allow BGP to support a gradual transition from 2-byte autonomous system numbers to 4-byte autonomous system numbers. A new reserved (private) autonomous system number, 23456, was created by RFC 4893 and this number cannot be configured as an autonomous system number in the Cisco IOS CLI.

RFC 5398, *Autonomous System (AS) Number Reservation for Documentation Use*, describes new reserved autonomous system numbers for documentation purposes. Use of the reserved numbers allow configuration examples to be accurately documented and avoids conflict with production networks if these configurations are literally copied. The reserved numbers are documented in the IANA autonomous system number registry. Reserved 2-byte autonomous system numbers are in the contiguous block, 64496 to 64511 and reserved 4-byte autonomous system numbers are from 65536 to 65551 inclusive.

Private 2-byte autonomous system numbers are still valid in the range from 64512 to 65534 with 65535 being reserved for special use. Private autonomous system numbers can be used for internal routing domains but must be translated for traffic that is routed out to the Internet. BGP should not be configured to advertise private autonomous system numbers to external networks. Cisco IOS software does not remove private autonomous system numbers from routing updates by default. We recommend that ISPs filter private autonomous system numbers.

Note Autonomous system number assignment for public and private networks is governed by the IANA. For information about autonomous-system numbers, including reserved number assignment, or to apply to register an autonomous system number, see the following URL: http://www.iana.org/.

Examples

The following example configures a BGP process for autonomous system 45000 and configures two external BGP neighbors in different autonomous systems using 2-byte autonomous system numbers:

```
router bgp 45000
 neighbor 192.168.1.2 remote-as 40000
 neighbor 192.168.3.2 remote-as 50000
 neighbor 192.168.3.2 description finance
 !
 address-family ipv4
  neighbor 192.168.1.2 activate
  neighbor 192.168.3.2 activate
  no auto-summary
  no synchronization
  network 172.17.1.0 mask 255.255.255.0
  exit-address-family
```

The following example configures a BGP process for autonomous system 65538 and configures two external BGP neighbors in different autonomous systems using 4-byte autonomous system numbers in asplain notation. This example is supported in Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases.

```
router bgp 65538
 neighbor 192.168.1.2 remote-as 65536
 neighbor 192.168.3.2 remote-as 65550
 neighbor 192.168.3.2 description finance
 !
 address-family ipv4
  neighbor 192.168.1.2 activate
  neighbor 192.168.3.2 activate
  no auto-summary
  no synchronization
  network 172.17.1.0 mask 255.255.255.0
  exit-address-family
```

The following example configures a BGP process for autonomous system 1.2 and configures two external BGP neighbors in different autonomous systems using 4-byte autonomous system numbers in asdot notation. This example is supported in Cisco IOS Release 12.0(32)SY8, 12.0(32)S12, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, 12.4(24)T, and Cisco IOS XE Release 2.3, and later releases.

```
router bgp 1.2
 neighbor 192.168.1.2 remote-as 1.0
 neighbor 192.168.3.2 remote-as 1.14
 neighbor 192.168.3.2 description finance
 !
 address-family ipv4
  neighbor 192.168.1.2 activate
  neighbor 192.168.3.2 activate
  no auto-summary
  no synchronization
  network 172.17.1.0 mask 255.255.255.0
  exit-address-family
```

Related Commands

Command	Description
bgp asnotation dot	Changes the default display and the regular expression match format of BGP 4-byte autonomous system numbers from asplain (decimal values) to dot notation.
neighbor remote-as	Adds an entry to the BGP or multiprotocol BGP neighbor table.
network (BGP and multiprotocol BGP)	Specifies the list of networks for the BGP routing process.

router ospfv3

To enter Open Shortest Path First version 3 (OSPFv3) router configuration mode , use the **router ospfv3** command in interface configuration mode.

router ospfv3 [*process-id*]

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.

Command Default

No OSPFv3 routing process is defined.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

Use the **router ospfv3** command to enter the OSPFv3 router configuration mode. From this mode, you can enter address-family configuration mode for IPv6 or IPv4 and then configure the IPv6 or IPv4 AF.

Examples

The following example enters OSPFv3 router configuration mode:

```
Router(config)# router ospfv3 1
Router(config-router)#
```

Related Commands

Command	Description
ipv6 ospf area	Enables OSPFv3 on an interface
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

route-map

To define the conditions for redistributing routes from one routing protocol into another routing protocol, or to enable policy routing, use the **route-map** command in global configuration mode and the **match** and **set** commands in route-map configuration modes. To delete an entry, use the **no** form of this command.

route-map *map-tag* [**permit** | **deny**] [*sequence-number*]

no route-map *map-tag* [**permit** | **deny**] [*sequence-number*]

Syntax Description

map-tag	A meaningful name for the route map. The **redistribute** router configuration command uses this name to reference this route map. Multiple route maps may share the same map tag name.
permit	(Optional) If the match criteria are met for this route map, and the **permit** keyword is specified, the route is redistributed as controlled by the set actions. In the case of policy routing, the packet is policy routed. If the match criteria are not met, and the **permit** keyword is specified, the next route map with the same map tag is tested. If a route passes none of the match criteria for the set of route maps sharing the same name, it is not redistributed by that set.
deny	(Optional) If the match criteria are met for the route map and the **deny** keyword is specified, the route is not redistributed. In the case of policy routing, the packet is not policy routed, and no further route maps sharing the same map tag name will be examined. If the packet is not policy routed, the normal forwarding algorithm is used.
sequence-number	(Optional) Number that indicates the position a new route map will have in the list of route maps already configured with the same name. If used with the **no** form of this command, the position of the route map should be deleted.

Command Default

Policy routing is not enabled and conditions for redistributing routes from one routing protocol into another routing protocol are not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.3(7)T	This command was updated for use in configuring IPv6 policy-based routing (PBR).
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Release	Modification
Cisco IOS XE Release 2.1	This command was implemented on Cisco ASR 1000 Series Aggregation Services Routers.
12.2(33)SXI4	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SXI4.

Usage Guidelines

Use the **route-map** command to enter route-map configuration mode.

Use route maps to redistribute routes or to subject packets to policy routing. Both purposes are described in this section.

Redistribution

Use the **route-map** global configuration command, and the **match** and **set** route-map configuration commands, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the *set actions*—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **match** route-map configuration command has multiple formats. The **match** commands can be given in any order, and all **match** commands must "pass" to cause the route to be redistributed according to the *set actions* given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

Use route maps when you want detailed control over how routes are redistributed between routing processes. The destination routing protocol is the one you specify with the **router** global configuration command. The source routing protocol is the one you specify with the **redistribute** router configuration command. See the "Examples" section for an illustration of how route maps are configured.

When you are passing routes through a route map, a route map can have several parts. Any route that does not match at least one **match** clause relating to a **route-map** command will be ignored; that is, the route will not be advertised for outbound route maps and will not be accepted for inbound route maps. If you want to modify only some data, you must configure a second route map section with an explicit match specified.

Policy Routing

Another purpose of route maps is to enable policy routing. Use the **ip policy route-map** or **ipv6 policy route-map** command, in addition to the **route-map** command, and the **match** and **set** commands to define the conditions for policy routing packets. The **match** commands specify the conditions under which policy routing occurs. The **set** commands specify the routing actions to perform if the criteria enforced by the **match** commands are met. You might want to policy route packets some way other than the obvious shortest path.

The *sequence-number* argument works as follows:

1. If no entry is defined with the supplied tag, an entry is created with the *sequence-number* argument set to 10.
2. If only one entry is defined with the supplied tag, that entry becomes the default entry for the following **route-map** command. The *sequence-number* argument of this entry is unchanged.
3. If more than one entry is defined with the supplied tag, an error message is printed to indicate that the *sequence-number* argument is required.

If the **no route-map** *map-tag* command is specified (with no *sequence-number* argument), the whole route map is deleted.

Examples

The following example redistributes Routing Information Protocol (RIP) routes with a hop count equal to 1 into Open Shortest Path First (OSPF). These routes will be redistributed into OSPF as external link-state advertisements (LSAs) with a metric of 5, metric type of Type 1, and a tag equal to 1.

```
Router(config)# router ospf 109
Router(config-router)# redistribute rip route-map rip-to-ospf
Router(config-router)# exit
Router(config)# route-map rip-to-ospf permit
Router(config-route-map)# match metric 1
Router(config-route-map)# set metric 5
Router(config-route-map)# set metric-type type1
Router(config-route-map)# set tag 1
```

The following example for IPv6 redistributes RIP routes with a hop count equal to 1 into OSPF. These routes will be redistributed into OSPF as external LSAs with a tag equal to 42 and a metric type equal to type1.

```
Router(config)# ipv6 router ospf 1
Router(config-router)# redistribute rip one route-map rip-to-ospfv3
Router(config-router)# exit
Router(config)# route-map rip-to-ospfv3
Router(config-route-map)# match tag 42
Router(config-route-map)# set metric-type type1
```

The following named configuration example redistributes Enhanced Interior Gateway Routing Protocol (EIGRP) addresses with a hop count equal to 1. These addresses are redistributed into EIGRP as external with a metric of 5 and a tag equal to 1:

```
Router(config)# router eigrp virtual-name1
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# topology base
Router(config-router-af-topology)# redistribute eigrp 6473 route-map
virtual-name1-to-virtual-name2
Router(config-router-af-topology)# exit-address-topology
Router(config-router-af)# exit-address-family
Router(config-router)# router eigrp virtual-name2
Router(config-router)# address-family ipv4 autonomous-system 6473
Router(config-router-af)# topology base
Router(config-router-af-topology)# exit-af-topology
Router(config-router-af)# exit-address-family
Router(config)# route-map virtual-name1-to-virtual-name2
Router(config-route-map)# match tag 42
Router(config-route-map)# set metric 5
Router(config-route-map)# set tag 1
```

Related Commands

Command	Description
ip policy route-map	Identifies a route map to use for policy routing on an interface.
ipv6 policy route-map	Configures IPv6 PBR on an interface.
match as-path	Matches a BGP autonomous system path access list.
match community	Matches a BGP community.
match interface (IP)	Distributes any routes that have their next hop out one of the interfaces specified.

Command	Description
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match ipv6 address	Distributes IPv6 routes that have a prefix permitted by a prefix list or to specify an IPv6 access list to use to match packets for PBR for IPv6.
match ip next-hop	Redistributes any routes that have a next hop router address passed by one of the access lists specified.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match length	Bases policy routing on the Level 3 length of a packet.
match metric (IP)	Redistributes routes with the metric specified.
match route-type (IP)	Redistributes routes of the specified type.
match tag	Redistributes routes in the routing table that match the specified tags.
router eigrp	Configures the EIGRP address-family process.
set as-path	Modifies an autonomous system path for BGP routes.
set automatic-tag	Automatically computes the tag value.
set community	Sets the BGP communities attribute.
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Indicates where to output packets that pass a match clause of a route map for policy routing.
set ipv6 default next-hop	Specifies an IPv6 default next hop to which matching packets will be forwarded.
set ip default next-hop verify-availability	Indicates where to output packets that pass a match clause of a route map for policy routing and for which the Cisco IOS software has no explicit route to a destination.
set ip next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing.
set ipv6 next-hop (PBR)	Indicates where to output IPv6 packets that pass a match clause of a route map for PBR for IPv6.
set level (IP)	Indicates where to import routes.
set local preference	Specifies a preference value for the autonomous system path.
set metric (BGP, OSPF, RIP)	Sets the metric value for a routing protocol.
set metric type	Sets the metric type for the destination routing protocol.
set next-hop	Specifies the address of the next hop.
set tag (IP)	Sets a tag value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.
show route-map	Displays all route maps configured or only the one specified.