I through R

ip authentication key-chain eigrp

To enable authentication of Enhanced Interior Gateway Routing Protocol (EIGRP) packets, use the **ip authentication key-chain eigrp**command in interface configuration mode. To disable such authentication, use the **no** form of this command.

ip authentication key-chain eigrp *as-number key-chain*

no ip authentication key-chain eigrp *as-number key-chain*

Syntax Description

as-number	Autonomous system number to which the authentication applies.
key-chain	Name of the authentication key chain.

Command Default

No authentication is provided for EIGRP packets.

Command Modes

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

Command History

Release	Modification
11.2F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Examples

The following example applies authentication to autonomous system 2 and identifies a key chain named SPORTS:

```
ip authentication key-chain eigrp 2 SPORTS
```

Related Commands

Command	Description
accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.
ip authentication mode eigrp	Specifies the type of authentication used in EIGRP packets.
key	Identifies an authentication key on a key chain.
key chain	Enables authentication of routing protocols.
key-string (authentication)	Specifies the authentication string for a key.
send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.

ip authentication mode eigrp

To specify the type of authentication used in Enhanced Interior Gateway Routing Protocol (EIGRP) packets, use the **ip authentication mode eigrp**command in interface configuration mode. To disable that type of authentication, use the **no** form of this command.

ip authentication mode eigrp *as-number* **md5**

no ip authentication mode eigrp *as-number* **md5**

Syntax Description

as-number	Autonomous system number.
md5	Keyed Message Digest 5 (MD5) authentication.

Command Default

No authentication is provided for EIGRP packets.

Command Modes

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

Command History

Release	Modification
11.2F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

Configure authentication to prevent unapproved sources from introducing unauthorized or false routing messages. When authentication is configured, an MD5 keyed digest is added to each EIGRP packet in the specified autonomous system.

Examples

The following example configures the interface to use MD5 authentication in EIGRP packets in autonomous system 10:

```
ip authentication mode eigrp 10 md5
```

Related Commands

Command	Description
accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.
ip authentication key-chain eigrp	Enables authentication of EIGRP packets.
key	Identifies an authentication key on a key chain.
key chain	Enables authentication of routing protocols.
key-string (authentication)	Specifies the authentication string for a key.
send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.

ipv6 authentication mode eigrp

To specify the type of authentication used in Enhanced Interior Gateway Routing Protocol (EIGRP) packets for IPv6, use the **ipv6 authentication mode eigrp**command in interface configuration mode. To disable the type of authentication, use the **no** form of this command.

ipv6 authentication mode eigrp *as-number* **md5**

no ipv6 authentication mode eigrp *as-number* **md5**

Syntax Description

as-number	Autonomous system number.
md5	Specifies keyed message digest 5 (MD5) authentication.

Command Default

No authentication is provided for EIGRP for IPv6 packets.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

Use the **ipv6 authentication mode eigrp**command to configure authentication to prevent unapproved sources from introducing unauthorized or false routing messages. When authentication is configured, an MD5 keyed digest is added to each EIGRP for IPv6 packet in the specified autonomous system.

Examples

The following example configures the interface to use MD5 authentication in EIGRP for IPv6 packets in autonomous system 1:

```
Router(config-if)# ipv6 authentication mode eigrp 1 md5
```

Related Commands

Command	Description
accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.
ipv6 authentication key-chain eigrp	Enables authentication of EIGRP packets for IPv6.
key	Identifies an authentication key on a key chain.
key chain	Enables authentication of routing protocols.
key-string (authentication)	Specifies the authentication string for a key.
send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.

ip bandwidth-percent eigrp

To configure the percentage of bandwidth that may be used by Enhanced Interior Gateway Routing Protocol (EIGRP) on an interface, use the **ip bandwidth-percent eigrp**command in interface configuration mode. To restore the default value, use the **no** form of this command.

ip bandwidth-percent eigrp *as-number percent*

no ip bandwidth-percent eigrp *as-number percent*

Syntax Description

as-number	Autonomous system number.
percent	Percent of bandwidth that EIGRP may use.

Command Default

EIGRP may use 50 percent of available bandwidth.

Command Modes

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

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

EIGRP will use up to 50 percent of the bandwidth of a link, as defined by the **bandwidth** interface configuration command. This command may be used if some other fraction of the bandwidth is desired. Note that values greater than 100 percent may be configured. The configuration option may be useful if the bandwidth is set artificially low for other reasons.

Examples

The following example allows EIGRP to use up to 75 percent (42 kbps) of a 56-kbps serial link in autonomous system 209:

```
Router(config)# interface serial 0
Router(config-if)# bandwidth 56
Router(config-if)# ip bandwidth-percent eigrp 209 75
```

Related Commands

Command	Description
bandwidth (interface)	Sets a bandwidth value for an interface.

ip hello-interval eigrp

To configure the hello interval for an Enhanced Interior Gateway Routing Protocol (EIGRP) process, use the **ip hello-interval eigrp** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ip hello-interval eigrp *as-number seconds*

no ip hello-interval eigrp *as-number* [*seconds*]

Syntax Description

as-number	Autonomous system number.
seconds	Hello interval (in seconds). The range is from 1 to 65535.

Command Default

The hello interval for low-speed, nonbroadcast multiaccess (NBMA) networks is 60 seconds and 5 seconds for all other networks.

Command Modes

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

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

The default of 60 seconds applies only to low-speed, NBMA media. Low speed is considered to be a rate of T1 or slower, as specified with the **bandwidth** interface configuration command. Note that for the purposes of EIGRP, Frame Relay and Switched Multimegabit Data Service (SMDS) networks may be considered to be NBMA. These networks are considered NBMA if the interface has not been configured to use physical multicasting; otherwise, they are considered not to be NBMA.

Examples

The following example sets the hello interval for Ethernet interface 0 to 10 seconds:

```
Router(config)# interface ethernet 0
Router(config-if)# ip hello-interval eigrp 109 10
```

Related Commands

Command	Description
bandwidth (interface)	Sets a bandwidth value for an interface.
ip hold-time eigrp	Configures the hold time for a particular EIGRP routing process designated by the autonomous system number.

ip hold-time eigrp

To configure the hold time for an Enhanced Interior Gateway Routing Protocol (EIGRP) process, use the **ip hold-time eigrp** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ip hold-time eigrp *as-number seconds*

no ip hold-time eigrp *as-number seconds*

Syntax Description

as-number	Autonomous system number.
seconds	Hold time (in seconds). The range is from 1 to 65535.

Command Default

The EIGRP hold time is 180 seconds for low-speed, nonbroadcast multiaccess (NBMA) networks and 15 seconds for all other networks.

Command Modes

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

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

On very congested and large networks, the default hold time might not be sufficient time for all routers and access servers to receive hello packets from their neighbors. In this case, you may want to increase the hold time.

We recommend that the hold time be at least three times the hello interval. If a router does not receive a hello packet within the specified hold time, routes through this router are considered unavailable.

Increasing the hold time delays route convergence across the network.

The default of 180 seconds hold time and 60 seconds hello interval apply only to low-speed, NBMA media. Low speed is considered to be a rate of T1 or slower, as specified with the **bandwidth** interface configuration command.

Examples

The following example sets the hold time for Ethernet interface 0 to 40 seconds:

```
Router(config)# interface ethernet 0
Router(config-if)# ip hold-time eigrp 109 40
```

Related Commands

Command	Description
bandwidth (interface)	Sets a bandwidth value for an interface.
ip hello-interval eigrp	Configures the hello interval for the EIGRP routing process designated by an autonomous system number.

ip next-hop-self eigrp

To enable the Enhanced Interior Gateway Routing Protocol (EIGRP) to advertise routes with the local outbound interface address as the next hop, use the **ip next-hop-self eigrp** command in interface configuration mode or virtual network interface mode. To instruct EIGRP to use the received next hop instead of the local outbound interface address, use the **no** form of this command.

ip next-hop-self eigrp *autonomous-system-number*

no ip next-hop-self eigrp *autonomous-system-number*[**no-ecmp-mode**]

Syntax Description

autonomous-system-number	Autonomous system number.
no-ecmp-mode	(Optional) Evaluates all paths to a network before advertising the paths out of an interface.

Command Default

The IP next-hop-self state is enabled.

Command Modes

Interface configuration (config-if)

Virtual network interface (config-if-vnet)

Command History

Release	Modification
12.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 3.2S	This command was modified. This command was made available in virtual network interface configuration mode.
Cisco IOS XE Release 3.5S	This command was modified. The **no-ecmp-mode** keyword was added.
15.2(1)S	This command was modified. The **no-ecmp-mode** keyword was added.
15.2(3)T	This command was modified. The **no-ecmp-mode** keyword was added.

Usage Guidelines

EIGRP, by default, sets the next-hop value to the local outbound interface address for routes that it is advertising, even when advertising those routes back out of the same interface on which they were learned. To change this default, you must use the **no ip next-hop-self eigrp** interface configuration command to instruct EIGRP to use the received next-hop value when advertising these routes. Following are some exceptions to this guideline:

- If your topology does not require spoke-to-spoke dynamic tunnels, you need not configure the **no ip next-hop-self eigrp** command.
- If your topology requires spoke-to-spoke dynamic tunnels, you must use process switching on the tunnel interface of spoke devices. Otherwise, you will need to use a different routing protocol over Dynamic Multipoint VPN (DMVPN).

The **no-ecmp-mode** option is an enhancement to the **no ip next-hop-self eigrp** command. When this option is enabled, all routes to a network in the EIGRP table are evaluated to check whether routes advertised from an interface were learned on the same interface. If a route advertised by an interface was learned on the same interface, the **no ip next-hop-self eigrp** configuration is honored and the received next hop is used to advertise this route. Disabling the IP next-hop self functionality is primarily useful in DMVPN spoke-to-spoke topologies.

Examples

The following example shows how to change the default next-hop value in IPv4 classic mode configurations by disabling the **ip next-hop-self** functionality and configuring EIGRP to use the received next-hop value to advertise routes:

```
Device(config)# interface tun 0
Device(config-if)# no ip next-hop-self eigrp 101 no-ecmp-mode
```

Related Commands

Command	Description
ipv6 next-hop self eigrp	Instructs an EIGRP device that the IPv6 next hop is the local outbound interface.
next-hop-self	Enables EIGRP to advertise routes with the local outbound interface address as the next hop.

ip split-horizon eigrp

To enable Enhanced Interior Gateway Routing Protocol (EIGRP) split horizon, use the **ip split-horizon eigrp** command in interface configuration mode. To disable split horizon, use the **no** form of this command.

ip split-horizon eigrp *as-number*

no ip split-horizon eigrp *as-number*

Syntax Description

as-number	Autonomous system number.

Command Default

The behavior of this command is enabled by default.

Command Modes

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

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

For networks that include links over X.25 packet-switched networks (PSNs), you can use the **neighbor** router configuration command to defeat the split horizon feature. As an alternative, you can explicitly specify the **no ip split-horizon eigrp** command in your configuration. However, if you do so, you must similarly disable split horizon for all routers and access servers in any relevant multicast groups on that network.

Note In general, we recommend that you not change the default state of split horizon unless you are certain that your application requires the change in order to properly advertise routes. Remember that if split horizon is disabled on a serial interface and that interface is attached to a packet-switched network, you must disable split horizon for all routers and access servers in any relevant multicast groups on that network.

Examples

The following example disables split horizon on a serial link connected to an X.25 network:

```
interface serial 0
 encapsulation x25
 no ip split-horizon eigrp 101
```

Related Commands

Command	Description
ip split-horizon (RIP)	Enables the split horizon mechanism.
neighbor (EIGRP)	Defines a neighboring router with which to exchange routing information.

ip summary-address eigrp

To configure address summarization for the Enhanced Interior Gateway Routing Protocol (EIGRP) on a specified interface, use the **ip summary-address eigrp** command in interface configuration or virtual network interface configuration mode. To disable the configuration, use the **no** form of this command.

ip summary-address eigrp *as-number ip-address mask* [*admin-distance*] [**leak-map** *name*]

no ip summary-address eigrp *as-number ip-address mask*

Syntax Description

as-number	Autonomous system number.
ip-address	Summary IP address to apply to an interface.
mask	Subnet mask.
admin-distance	(Optional) Administrative distance. Range: 0 to 255. **Note** Starting with Cisco IOS XE Release 3.2S, the *admin-distance* argument was removed. Use the **summary-metric** command to configure the administrative distance.
leak-map *name*	(Optional) Specifies the route-map reference that is used to configure the route leaking through the summary.

Command Default

- An administrative distance of 5 is applied to EIGRP summary routes.
- EIGRP automatically summarizes to the network level, even for a single host route.
- No summary addresses are predefined.
- The default administrative distance metric for EIGRP is 90.

Command Modes

Interface configuration (config-if)

Virtual network interface configuration (config-if-vnet)

Command History

Release	Modification
10.0	This command was introduced.
12.0(7)T	This command was modified. The *admin-distance* argument was added.
12.3(14)T	This command was modified. The **leak-map** keyword was added.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode. The *admin-distance* argument was removed. Use the **summary-metric** command to configure the administrative distance.
12.2(33)SXJ	This command was modified. The summary address is not advertised to the peer if the administrative distance is configured as 255.
15.0(1)SY	This command was modified. Support was added for this command in virtual network interface configuration mode.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.

Usage Guidelines

The **ip summary-address eigrp** command is used to configure interface-level address summarization. EIGRP summary routes are given an administrative-distance value of 5. The administrative-distance metric is used to advertise a summary without installing it in the routing table.

By default, EIGRP summarizes subnet routes to the network level. The **no auto-summary** command can be entered to configure the subnet-level summarization.

The summary address is not advertised to the peer if the administrative distance is configured as 255.

EIGRP Support for Leaking Routes

Configuring the **leak-map** keyword allows a component route that would otherwise be suppressed by the manual summary to be advertised. Any component subset of the summary can be leaked. A route map and access list must be defined to source the leaked route.

The following is the default behavior if an incomplete configuration is entered:

- If the **leak-map** keyword is configured to reference a nonexistent route map, the configuration of this keyword has no effect. The summary address is advertised but all component routes are suppressed.
- If the **leak-map** keyword is configured but the access list does not exist or the route map does not reference the access list, the summary address and all component routes are advertised.

If you are configuring a virtual-network trunk interface and you configure the **ip summary-address eigrp** command, the *admin-distance* value of the command is not inherited by the virtual networks running on the trunk interface because the administrative distance option is not supported in the **ip summary-address eigrp** command on virtual network subinterfaces.

Examples

The following example shows how to configure an administrative distance of 95 on Ethernet interface 0/0 for the 192.168.0.0/16 summary address:

```
Router(config)# router eigrp 1
Router(config-router)# no auto-summary
Router(config-router)# exit
Router(config)# interface Ethernet 0/0
Router(config-if)# ip summary-address eigrp 1 192.168.0.0 255.255.0.0 95
```

The following example shows how to configure the 10.1.1.0/24 subnet to be leaked through the 10.2.2.0 summary address:

```
Router(config)# router eigrp 1
Router(config-router)# exit
Router(config)# access-list 1 permit 10.1.1.0 0.0.0.255
Router(config)# route-map LEAK-10-1-1 permit 10
Router(config-route-map)# match ip address 1
Router(config-route-map)# exit
Router(config)# interface Serial 0/0
Router(config-if)# ip summary-address eigrp 1 10.2.2.0 255.0.0.0 leak-map LEAK-10-1-1
Router(config-if)# end
```

The following example configures GigabitEthernet interface 0/0/0 as a virtual network trunk interface:

```
Router(config)# interface gigabitethernet 0/0/0
Router(config-if)# vnet global
Router(config-if-vnet)# ip summary-address eigrp 1 10.3.3.0 255.0.0.0 33
```

Related Commands

Command	Description
auto-summary (EIGRP)	Configures automatic summarization of subnet routes to network-level routes (default behavior).
summary-metric	Configures fixed metrics for an EIGRP summary aggregate address.

ipv6 authentication key-chain eigrp

To enable authentication of Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 packets, use the **ipv6 authentication key-chain eigrp**command in interface configuration mode. To disable authentication of EIGRP for IPv6 packets, use the **no** form of this command.

ipv6 authentication key-chain eigrp *as-number key-chain*

no ipv6 authentication key-chain eigrp *as-number key-chain*

Syntax Description

as-number	Autonomous system number.
key-chain	Name of the authentication key chain.

Command Default

No authentication is provided for EIGRP for IPv6 packets.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

EIGRP for IPv6 route authentication provides Message Digest 5 (MD5) authentication of routing updates from the EIGRP for IPv6 routing protocol. The MD5 keyed digest in each EIGRP for IPv6 packet prevents the introduction of unauthorized or false routing messages from unapproved sources.

Each key has its own key identifier, which is stored locally. The combination of the key identifier and the interface associated with the message uniquely identifies the authentication algorithm and MD5 authentication key in use.

You can configure multiple keys with lifetimes. Only one authentication packet is sent, regardless of how many valid keys exist. The software examines the key numbers in order from lowest to highest, and uses the first valid key it encounters.

Examples

The following example enables authentication for EIGRP for IPv6 for AS 1, using a key chain named chain1:

```
Router(config-if)# ipv6 authentication key-chain eigrp 1 chain1
```

Related Commands

Command	Description
accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.
ipv6 authentication mode eigrp	Specifies the type of authentication used in EIGRP for IPv6 packets.
key	Identifies an authentication key on a key chain.
key chain	Enables authentication of routing protocols.
key-string (authentication)	Specifies the authentication string for a key.
send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.

ipv6 bandwidth-percent eigrp

To configure the percentage of bandwidth that may be used by Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 on an interface, use the **ipv6 bandwidth-percent eigrp**command in interface configuration mode. To restore the default value, use the **no** form of this command.

ipv6 bandwidth-percent eigrp *as-number percent*

no ipv6 bandwidth-percent eigrp *as-number percent*

Syntax Description

as-number	Autonomous system number.
percent	Percentage of bandwidth that EIGRP for IPv6 may use.

Command Default

Percentage of bandwidth used is 50 percent.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

EIGRP for IPv6 uses as much as 50 percent of the bandwidth of a link, as defined by the **bandwidth** command. The ipv6 bandwidth-percent eigrp command may be used if some other fraction of the bandwidth is desired.

Note that values greater than 100 percent may be configured. The configuration option may be useful if the bandwidth is set artificially low for other reasons.

Examples

The following example allows EIGRP for IPv6 to use up to 75 percent (42 kbps) of a 56-kbps serial link in autonomous system 1:

```
interface serial 0
 bandwidth 56
 ipv6 bandwidth-percent eigrp 1 75
```

Related Commands

Command	Description
bandwidth (interface)	Sets a bandwidth value for an interface.

ipv6 eigrp

To enable Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 on a specified interface, use the **ipv6 eigrp** command in interface configuration mode. To disable EIGRP for IPv6, use the **no** form of this command.

ipv6 eigrp *as-number*

no ipv6 eigrp *as-number*

Syntax Description

as-number	Autonomous system number.

Command Default

EIGRP is not enabled on an IPv6 interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Use the **ipv6 eigrp** command to enable EIGRP for IPv6 on a per-interface basis.

If an autonomous system is specified, EIGRP for IPv6 is enabled only for the specified autonomous system. Otherwise, EIGRP for IPv6 is specified throughout the interface.

Examples

The following example enables EIGRP for IPv6 for AS 1 on Ethernet interface 0:

```
Router(config)# interface ethernet0
Router(config-if)# ipv6 eigrp 1
```

Related Commands

Command	Description
ipv6 enable	Enables IPv6 processing on an interface that has not been configured with an explicit IPv6 address.
ipv6 router eigrp	Configures the EIGRP routing process in IPv6.

ipv6 hello-interval eigrp

To configure the hello interval for the Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 routing process designated by an autonomous system number, use the **ipv6 hello-interval eigrp** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ipv6 hello-interval eigrp *as-number seconds*

no ipv6 hello-interval eigrp *as-number seconds*

Syntax Description

as-number	Autonomous system number.
seconds	Hello interval, in seconds. The range is from 1 to 65535.

Command Default

For low-speed, nonbroadcast multiaccess (NBMA) networks, the default hello interval is 60 seconds. For all other networks, the default hello interval is 5 seconds.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

The default of 60 seconds applies only to low-speed, NBMA media. Low speed is considered to be a rate of T1 or slower, as specified with the **bandwidth** interface configuration command. Note that for the purposes of EIGRP for IPv6, Frame Relay and Switched Multimegabit Data Service (SMDS) networks may be considered to be NBMA. These networks are considered NBMA if the interface has not been configured to use physical multicasting; otherwise, they are considered not to be NBMA.

Examples

The following example sets the hello interval for Ethernet interface 0 to 10 seconds on autonomous system 1:

```
interface ethernet 0
 ipv6 hello-interval eigrp 1 10
```

Related Commands

Command	Description
bandwidth (interface)	Sets a bandwidth value for an interface.
ipv6 hold-time eigrp	Configures the hold time for a particular EIGRP for IPv6 routing process designated by the autonomous system number.

ipv6 hold-time eigrp

To configure the hold time for a particular Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 routing process designated by the autonomous system number, use the **ipv6 hold-time eigrp**command in interface configuration mode. To restore the default value, use the **no** form of this command.

ipv6 hold-time eigrp *as-number seconds*

no ipv6 hold-time eigrp *as-number seconds*

Syntax Description

as-number	Autonomous system number.
seconds	Hello interval, in seconds. The range is from 1 to 65535.

Command Default

For low-speed, nonbroadcast multiaccess (NBMA) networks, the default hold-time interval is 180 seconds. For all other networks, the default hold-time interval is 15 seconds.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

On very congested and large networks, the default hold time might not be sufficient time for all routers and access servers to receive hello packets from their neighbors. In this case, you may want to increase the hold time.

Cisco recommends that the hold time be at least three times the hello interval. If a router does not receive a hello packet within the specified hold time, routes through this router are considered unavailable.

Increasing the hold time delays route convergence across the network.

The default of 180 seconds hold time and 60 seconds hello interval apply only to low-speed, NBMA media. Low speed is considered to be a rate of T1 or slower, as specified with the **bandwidth** command.

Examples

The following example sets the hold time for Ethernet interface 0 to 40 seconds for AS 1:

```
interface ethernet 0
 ipv6 hold-time eigrp 1 40
```

Related Commands

Command	Description
bandwidth (interface)	Sets a bandwidth value for an interface.
ipv6 hello-interval eigrp	Configures the hello interval for the EIGRP for IPv6 routing process designated by an autonomous system number.

ipv6 next-hop-self eigrp

To instruct a device configured with the Enhanced Interior Gateway Routing Protocol (EIGRP) that the IPv6 next hop is the local outbound interface address, use the **ipv6 next-hop-self eigrp** command in interface configuration mode. To instruct EIGRP to use the received next hop instead of the local outbound interface, use the **no** form of this command.

ipv6 next-hop-self eigrp *as-number*

no ipv6 next-hop-self eigrp *as-number*[**no-ecmp-mode**]

Syntax Description

as-number	Autonomous system number.
no-ecmp-mode	(Optional) Evaluates all paths to a network before advertising the paths out of an interface.

Command Default

The IPv6 next-hop-self state is enabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.2(1)S	This command was integrated into Cisco IOS Release 15.2(1)S. The **no-ecmp-mode** keyword was added.
Cisco IOS XE Release 3.5S	This command was modified. The **no-ecmp-mode** keyword was added.
15.2(3)T	This command was modified. The **no-ecmp-mode** keyword was added.

Usage Guidelines

EIGRP, by default, sets the next-hop value to the local outbound interface address for routes that it is advertising, even when advertising those routes back out of the same interface on which they were learned. To change this default, use the **no ipv6 next-hop-self eigrp** command to instruct EIGRP to use the received next-hop value when advertising these routes. Some exceptions to this guideline are as follows:

- If your topology does not require spoke-to-spoke dynamic tunnels, you need not configure the **no ipv6 next-hop-self eigrp** command.
- If your topology requires spoke-to-spoke dynamic tunnels, you must use process switching on the tunnel interface on spoke devices. Otherwise, you will need to use a different routing protocol over Dynamic Multipoint VPN (DMVPN).

The **no-ecmp-mode** option is an enhancement to the **no ipv6 next-hop-self eigrp** command. When this option is enabled, all routes to a network in the EIGRP table are evaluated to check whether routes advertised from an interface were learned on the same interface. If a route advertised by an interface was learned on the same interface, the **no ipv6 next-hop-self eigrp** configuration is honored and the received next hop is used to advertise this route. Disabling the IPv6 next-hop self functionality is primarily useful in DMVPN spoke-to-spoke topologies.

Examples

The following example shows how to change the default IPv6 next-hop value by disabling the **ipv6 next-hop-self** functionality and configuring EIGRP to use the received next-hop value to advertise routes:

```
Device(config)# interface serial 0
Device(config-if)# no ipv6 next-hop-self eigrp 1 no-ecmp-mode
```

Related Commands

Command	Description
next-hop-self	Instructs an EIGRP device that the IPv6 next hop is the local outbound interface.
ip next-hop-self eigrp	Enables EIGRP to advertise routes with the local outbound interface address as the next hop.

ipv6 router eigrp

To place the router in router configuration mode, create an Enhanced Interior Gateway Routing Protocol (EIGRP) routing process in IPv6, and configure this process, use the **ipv6**router **eigrp**command in global configurationmode. To shut down a routing process, use the **no** form of this command.

ipv6 router eigrp *as-number* [**eigrp event-log-size event-log-size**]

no ipv6 router eigrp *as-number*

Syntax Description

as-number	Autonomous system number.
eigrp event-log-size *event-log-size*	(Optional) Memory allocation value of the EIGRP event. The *event-log-size* value is the memory allocation, in bytes, calculated dynamically based on available memory. The *event-log-size* value is between 0 and the dynamically calculated number.

Command Default

This command is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SRB	The **eigrp event-log-size** keyword and *event-log-size* argument were added.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

Use the **ipv6 router eigrp** command in global configuration mode to place the router in router configuration mode and create a routing process. Once in router configuration mode, you can configure the EIGRP for IPv6 routing process using the **ipv6 router eigrp** command.

Examples

The following example places the router in router configuration mode and allows you to configure an EIGRP for IPv6 routing process:

```
Router(config)# ipv6 router eigrp 400
```

```
eigrp router-id 10.13.14.15
eigrp stub connected summary
eigrp event-log-size 1000
no shutdown
```

Related Commands

Command	Description
ipv6 eigrp	Enables EIGRP for IPv6 on a specified interface.
router eigrp	Configures the EIGRP process.

ipv6 split-horizon eigrp

To enable Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 split horizon, use the **ipv6**split-horizon **eigrp**command in interface configuration mode. To disable split horizon, use the **no** form of this command.

ipv6 split-horizon eigrp *as-number*

no ipv6 split-horizon eigrp *as-number*

Syntax Description

as-number	Autonomous system number.

Command Default

EIGRP for IPv6 split horizon is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

For networks that include links over X.25 packet-switched networks (PSNs), you can use the **neighbor** command in router configuration mode to disable the split horizon feature. Or, you can specify the **no ipv6 split-horizon eigrp** command in your configuration. However, if you do disable the split horizon feature, you must similarly disable split horizon for all routers and access servers in any relevant multicast groups on that network.

Note In general, we recommend that you not change the default state of split horizon unless you are certain that your application requires the change in order to advertise routes properly. Remember that if split horizon is disabled on a serial interface and that interface is attached to a packet-switched network, you must disable split horizon for all routers and access servers in any relevant multicast groups on that network.

Examples

The following example disables split horizon on a serial link connected to an X.25 network:

```
interface serial 0
 encapsulation x25
 no ipv6 split-horizon eigrp 101
```

Related Commands

Command	Description
neighbor (EIGRP)	Defines a neighboring router with which to exchange routing information on a router that is running EIGRP.

ipv6 summary-address eigrp

To configure a summary aggregate address for a specified interface, use the **ipv6**summary-address **eigrp**command in interface configuration mode. To disable a configuration, use the **no** form of this command.

ipv6 summary-address eigrp *as-number ipv6-address* [*admin-distance*]

no ipv6 summary-address eigrp *as-number ipv6-address* [*admin-distance*]

Syntax Description

as-number	Autonomous system number.
ipv6-address	Summary IPv6 address to apply to an interface.
admin-distance	(Optional) Administrative distance. A value from 0 through 255. The default value is 90.

Command Default

An administrative distance of 5 is applied to Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 summary routes. EIGRP for IPv6 automatically summarizes to the network level, even for a single host route. No summary addresses are predefined.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **ipv6 summary-address eigrp** command is used to configure interface-level address summarization. EIGRP for IPv6 summary routes are given an administrative distance value of 5. The administrative distance metric is used to advertise a summary address without installing it in the routing table.

Examples

The following example provides a summary aggregate address for EIGRP for IPv6 for AS 1:

```
ipv6 summary-address eigrp 1 2001:0DB8:0:1::/64
```

log-neighbor-changes (EIGRP)

To enable the logging of changes in Enhanced Interior Gateway Routing Protocol (EIGRP) neighbor adjacencies, use the **log-neighbor-changes**command in IPX-router configuration mode. To disable this function, use the **no** form of this command.

log-neighbor-changes

no log-neighbor-changes

Syntax Description

This command has no arguments or keywords.

Command Default

No adjacency changes are logged.

Command Modes

IPX-router configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Enable the logging of neighbor adjacency changes in order to monitor the stability of the routing system and to help detect problems. Log messages are of the following form:

```
%DUAL-5-NBRCHANGE: IPX EIGRP
as-number
: Neighbor
address
(
interface
) is
state
:
reason
```

where the arguments have the following meanings:

as-number	Autonomous system number
address (interface)	Neighbor address
state	Up or down
reason	Reason for change

Examples The following configuration will log neighbor changes for EIGRP process 209:

```
ipx router eigrp 209
 log-neighbor-changes
```

log-neighbor-changes (IPv6 EIGRP)

To enable the logging of changes in Enhanced Interior Gateway Routing Protocol (EIGRP) IPv6 neighbor adjacencies, use the **log-neighbor-changes** command in router configuration mode. To disable the logging of changes in EIGRP IPv6 neighbor adjacencies, use the **no** form of this command.

log-neighbor-changes

no log-neighbor-changes

Syntax Description

This command has no arguments or keywords.

Command Default

Adjacency changes are logged.

Command Modes

Router configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The log-neighbor-changes command enables the logging of neighbor adjacency changes to monitor the stability of the routing system and to help detect problems.

Logging is enabled by default. To disable the logging of neighbor adjacency changes, use the no form of this command.

Examples

The following example disables logging of neighbor changes for EIGRP process 1:

```
ipv6 router eigrp 1
 no log-neighbor-changes
```

The following configuration enables logging of neighbor changes for EIGRP process 1:

```
ipv6 router eigrp 1
 log-neighbor-changes
```

Related Commands

Command	Description
log-neighbor- warnings	Enables the logging of EIGRP neighbor warning messages.

log-neighbor-warnings

Note Effective with Cisco IOS Release 15.0(1)M, 12.2(33)SRE and Cisco IOS XE Release 2.5, the **log-neighbor-warnings** command was replaced by the **eigrp log-neighbor-warnings** command for IPv4 and IPv6 configurations. The **log-neighbor-warnings** command is still available for IPX configurations.

To enable the logging of Enhanced Interior Gateway Routing Protocol (EIGRP) neighbor warning messages, use the **log-neighbor-warnings** command in router configuration mode. To disable the logging of EIGRP neighbor warning messages, use the **no** form of this command.

log-neighbor-warnings [*seconds*]

no log-neighbor-warnings

Syntax Description

seconds	(Optional) The time interval (in seconds) between repeated neighbor warning messages. The range of seconds is from 1 through 65535.

Command Default

Neighbor warning messages are logged.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.0(1)M	This command was replaced by the **eigrp log-neighbor-warnings** command for IPv4 and IPv6 configurations. The **log-neighbor-warnings** command is still available for IPX configurations.
12.2(33)SRE	This command was replaced by the **eigrp log-neighbor-warnings** command for IPv4 and IPv6 configurations. The **log-neighbor-warnings** command is still available for IPX configurations.

Release	Modification
Cisco IOS XE Release 2.5	This command was replaced by the **eigrp log-neighbor-warnings** command for IPv4 and IPv6 configurations. The **log-neighbor-warnings** command is still available for IPX configurations.

Usage Guidelines

When neighbor warning messages occur, they are logged by default. With the **log-neighbor-warnings** command, you can disable and enable the logging of neighbor warning messages and configure the interval between repeated neighbor warning messages.

Examples

The following example shows that neighbor warning messages will be logged for EIGRP process 1 and warning messages will be repeated in 5-minute (300 seconds) intervals:

```
Router(config)# ipv6 router eigrp 1
Router(config-router)# log-neighbor-warnings 300
```

Related Commands

Command	Description
log-neighbor-changes	Enables the logging of changes in EIGRP neighbor adjacencies.

match extcommunity

To match Border Gateway Protocol (BGP) or Enhanced Interior Gateway Routing Protocol (EIGRP) extended community list attributes, use the **match extcommunity** command in route-map configuration mode. To remove the **match extcommunity**command from the configuration file and remove the BGP or EIGRP extended community list attribute entry, use the **no** form of this command.

match extcommunity *extended-community-list-name*

no match extcommunity *extended-community-list-name*

Syntax Description

extended-community-list-name	Name of an extended community list.

Command Default

BGP and EIGRP extended community list attributes are not matched.

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
12.1	This command was introduced.
12.0(22)S	The maximum number of expanded extended community list numbers was changed from 199 to 500 in Cisco IOS Release 12.0(22)S.
12.2(15)T	The maximum number of expanded extended community list numbers was changed from 199 to 500 in Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2SX	This command is supported in the Cisco 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. Support for EIGRP was added.
12.2(33)SRE	This command was modified. Support for EIGRP was added.
Cisco IOS XE Release 2.5	This command was modified. Support for EIGRP was added.
12.2(33)XNE	This command was modified. Support for EIGRP was added.

Usage Guidelines

Extended community attributes are used to configure, filter, and identify routes for virtual routing and forwarding instances (VRFs) and Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs).

The **match extcommunity** command is used to configure match clauses that use extended community attributes in route maps. All of the standard rules of match and set clauses apply to the configuration of extended community attributes.

Examples

The following example shows that the routes that match extended community list 500 will have the weight set to 100. Any route that has extended community 1 will have the weight set to 100.

```
Router(config)# ip extcommunity-list 500 rt 100:2
Router(config-extcomm-list)# exit
Router(config)# route-map MAP_NAME permit 10
Router(config-route-map)# match extcommunity 1
Router(config-route-map)# set weight 100
```

Related Commands

Command	Description
ip extcommunity-list	Creates an extended community list for BGP and controls access to it.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another.
set extcommunity	Sets BGP extended community attributes.
set weight	Specifies the BGP weight for the routing table.
show ip extcommunity-list	Displays routes that are permitted by the extended community list.
show route-map	Displays configured route maps.

match tag list

To filter routes that match a specified route tag list, use the **match tag list** command in route-map configuration mode. To remove the route tag list entry, use the **no** form of this command.

match tag list *list-name* [*... list-name*]

no match tag list *list-name* [*... list-name*]

Syntax Description

list-name	Name of route tag lists.

Command Default

No match tag lists are defined.

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
15.2(2)S	This command was introduced.
Cisco IOS XE Release 3.6S	This command was integrated into Cisco IOS XE Release 3.6S.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.

Usage Guidelines

The ellipsis (...) in the command syntax indicates that the command input can include multiple values for the *list-name* argument. Route tag lists are used to filter routes. A single list can have multiple criteria for routes. Only routes that match all criteria specified in the route tag list are filtered.

The function of the **match tag list** command is similar to the **match tag** command; the **match tag** command specifies individual tag values and not tag lists.

Note You can use either the **match tag** command or the **match tag list** command but not both together within a single route-map sequence.

Examples

The following example shows how to filter routes from the route tag list named list1 by using the **match tag list** command:

```
Device(config)# route-map map1
Device(config-route-map)# match tag list list1
```

Related Commands

Command	Description
match tag	Filters routes that match specified route tags.
route-tag list	Creates a route tag list.
route-tag notation	Enables the display of route tag values in dotted decimal format.

maximum-prefix

To limit the number of prefixes that are accepted under an address family by an Enhanced Interior Gateway Routing Protocol (EIGRP) process, use the **maximum-prefix** command in address family configuration mode or address family topology configuration mode. To disable this function, use the **no** form of this command.

maximum-prefix *maximum* {[[*threshold*] **[dampened]** [**reset-time** *minutes*] [**restart** *minutes*] [**restart-count** *number*]]| **[warning-only]**}

no maximum-prefix

Syntax Description

maximum	Maximum number of prefixes allowed under an address family. The range for this argument is a number from 1 to 4294967295. **Note** The number of prefixes that can be configured is limited only by the available system resources on the router.
threshold	(Optional) The prefix percentage number. Valid values are 1 to 100. The default is 75. This value causes the router to generate syslog warning messages when the specified percentage of the maximum-prefix limit has been exceeded.
dampened	(Optional) Configures a decay penalty to be applied to the restart-time period each time the maximum-prefix limit is exceeded. The half-life for the decay penalty is 150 percent of the default or user-defined restart-time value in minutes. This keyword is disabled by default.
reset-time *minutes*	(Optional) Configures the router to reset the restart count to 0 after the default or user-defined reset-time period has expired. The range of values that can be applied with the *minutes* argument is from 1 to 65535 minutes. The default reset-time period is 15 minutes.
restart *minutes*	(Optional) Configures a time period in which the router will not form adjacencies or accept redistributed routes from the Routing Information Base (RIB) after the maximum-prefix limit has been exceeded. The value for the *minutes* argument is from 1 to 65535 minutes. The default restart-time period is 5 minutes.

restart-count *number*	(Optional) Configures the number of times a peering session can be automatically reestablished after the peering session has been torn down or after a redistribute route has been cleared and relearned because the maximum-prefix limit has been exceeded. The default restart-count limit is 3. **Caution** Once the restart count threshold has been crossed, you will need to enter the **clear ip route *** or **clear ip eigrp neighbor** command to reestablish normal peering and/or redistribution.
warning-only	(Optional) Configures the router to generate syslog messages only when the maximum-prefix limitis reached, instead of suspending peering session or route redistribution. This keyword is disabled by default.

Command Default

The number of prefixes that are accepted under an address family by an EIGRP process is not limited.

Command Modes

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

Command History

Release	Modification
12.0(29)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
15.0(1)M	This command was modified. Address family topology configuration mode was added for EIGRP named configurations.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

The **maximum-prefix** command is used to configure an EIGRP process to limit the number prefixes that are accepted from all sources. When the maximum-prefix limit is exceeded, sessions with remote peers are torn down, all routes learned from remote peers and through redistribution are removed from the topology and routing tables, and redistribution and peering is suspended for the default or user-defined time period.

Inherited Timer Values

Default or user-defined restart, restart-count, and reset-time values for the process-level configuration of this feature, configured with the **maximum-prefix** command, are inherited by the **redistribute maximum-prefix**

and **neighbor maximum-prefix** command configurations by default. If a single peer is configured with the **neighbor maximum-prefix** command, a process-level configuration or a configuration that is applied to all neighbors will be inherited.

Examples

The following example, starting in global configuration mode, configures the maximum prefix limit for an EIGRP process, which includes routes learned through redistribution and routes learned through EIGRP peering sessions. The maximum limit is set to 50000 prefixes. When the number of prefixes learned through redistribution reaches 37,500 (75 percent of 50,000), warning messages will be displayed in the console. When the maximum prefix limit is exceeded, all peering sessions will be reset, the topology and routing tables will be cleared and redistributed routes and all peering sessions will be placed in a penalty state.

```
Router(config)# router eigrp 100
Router(config-router)# address-family ipv4 vrf VRF1
Router(config-router-af)# maximum-prefix 50000

Router(config-router-af)# end
```

The following example configures the maximum prefix limit for an EIGRP named configuration process:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# topology base
Router(config-router-af-topology)# maximum-prefix 50000
```

Related Commands

Command	Description
clear ip eigrp neighbors	Deletes entries from the EIGRP neighbor table.
clear ip eigrp vrf neighbor	Deletes neighbor entries from the VRF table.
clear ip route	Deletes routes from the IP routing table.
neighbor maximum-prefix	Limits the number of prefixes that are accepted from a single EIGRP neighbor or from all EIGRP neighbors.
redistribute maximum-prefix	Limits the number of prefixes redistributed into an EIGRP process.

metric holddown

To keep new Enhanced Interior Gateway Routing Protocol (EIGRP) routing information from being used for a certain period of time, use the **metric holddown** command in router configuration mode. To disable this feature, use the **no** form of this command.

metric holddown

no metric holddown

Syntax Description

This command has no arguments or keywords.

Command Default

The holddown state is disabled.

Command Modes

Router configuration (config-router)

Command History

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

Usage Guidelines

The holddown state keeps new routing information from being used for a certain period of time. This function can prevent routing loops caused by slow convergence. It is sometimes advantageous to disable the holddown state to increase the ability of the network to quickly respond to topology changes; this command provides this function.

Use the **metric holddown** command if other routers or access servers within the EIGRP autonomous system are not configured with the **no metric holddown** command. If all routers are not configured the same way, you increase the possibility of routing loops.

Examples

The following example disables metric holddown:

```
Router(config)# router eigrp 15
Router(config-router)# network 172.16.0.0
Router(config-router)# network 192.168.7.0
Router(config-router)# no metric holddown
```

Related Commands

Command	Description
metric maximum-hops	Causes the IP routing software to advertise as unreachable those routes with a hop count higher than is specified by the command (EIGRP only).
metric weights (EIGRP)	Allows the tuning of the EIGRP metric calculations.

metric maximum-hops

To have the IP routing software advertise as unreachable routes with a hop count higher than is specified by the command (Enhanced Interior Gateway Routing Protocol [EIGRP] only), use the **metric maximum-hops** command in router configuration mode or address family topology configuration mode. Toreset the value to the default, use the **no** form of this command.

metric maximum-hops *hops-number*

no metric maximum-hops

Syntax Description

hops-number	Maximum hop count (in decimal). The default value is 100; the maximum number of hops that can be specified is 255.

Command Default

The maximum number of hops is 100.

Command Modes

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

Command History

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

Usage Guidelines

This command provides a safety mechanism that breaks any potential count-to-infinity problems. It causes the IP routing software to advertise as unreachable routes with a hop count greater than the value assigned to the *hops-number* argument.

Examples

In the following example, a router in autonomous system 71 attached to network 10.0.0.0 wants a maximum hop count of 200, doubling the default. The network administrators configured the router hop count to 200 because they have a complex WAN that can generate a large hop count under normal (nonlooping) operations.

```
Router(config)# router eigrp 71
Router(config-router)# network 172.16.0.0
Router(config-router)#
metric maximum-hops 200
```

The following example shows how to configure EIGRP autonomous-system 4453 to have a maximum hop count of 200:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# topology base
Router(config-router-af-topology)# metric maximum-hops 200
```

Related Commands

Command	Description
address-family (EIGRP)	Enters address-family configuration mode to configure an EIGRP routing instance.
metric holddown	Keeps new EIGRP routing information from being used for a certain period of time.
metric weights (EIGRP)	Allows the tuning of the EIGRP metric calculations.
network (EIGRP)	Specifies the network for an EIGRP routing process.
router eigrp	Configures the EIGRP address-family process.
topology (EIGRP)	Configures an EIGRP process to route IP traffic under the specified topology instance and enters address-family topology configuration mode.

metric rib-scale

To set the Routing Information Base (RIB) scaling factor for the Enhanced Interior Gateway Routing Protocol (EIGRP), use the **metric rib-scale** command in address family configuration mode. To remove the metric value and restore the default state, use the **no** form of this command.

metric rib-scale *scale-value*

no metric rib-scale *scale-value*

Syntax Description

scale-value	Scaling value for the RIB installation. The range is from 1 to 255. The default value is 128.

Command Default

The RIB scaling factor is set to 128.

Command Modes

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(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY

Usage Guidelines

Use the **metric rib-scale** command to clear all EIGRP routes and replace them with new metric values in the RIB.

Examples

The following example shows how to set the RIB-scale value to 100:

```
Router# configure terminal
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4533
Router(config-router-af)# metric rib-scale 100
```

Related Commands

Command	Description
metric weights (EIGRP)	Tunes EIGRP metric calculations.

metric weights (EIGRP)

To tune the Enhanced Interior Gateway Routing Protocol (EIGRP) metric calculations, use the **metric weights** command in router configuration mode or address family configuration mode. To reset the values to their defaults, use the **no** form of this command.

Router Configuration

metric weights *tos k1 k2 k3 k4 k5*

no metric weights

Address Family Configuration

metric weights *tos* [*k1* [*k2* [*k3* [*k4* [*k5* [*k6*]]]]]]

no metric weights

Syntax Description

tos	Type of service. This value must always be zero.
k1 k2 k3 k4 k5 k6	(Optional) Constants that convert an EIGRP metric vector into a scalar quantity. Valid values are 0 to 255. Given below are the default values: • *k1:* 1 • *k2:* 0 • *k3:* 1 • *k4:* 0 • *k5:* 0 • *k6:* 0 **Note** In address family configuration mode, if the values are not specified, default values are configured. The *k6* argument is supported only in address family configuration mode.

Command Default

EIGRP metric K values are set to their default values.

Command Modes

Router configuration (config-router)

Address family configuration (config-router-af)

Command History

Release	Modification
10.0	This command was introduced.
12.4(6)T	This command was modified. Support for IPv6 was added.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SRE	This command was modified. The address family configuration mode was added.
15.0(1)M	This command was modified. The address family configuration mode was added.
Cisco IOS XE Release 2.5	This command was modified. The address family configuration mode was added.
15.1(3)S	This command was modified. The *k6* argument was added.
Cisco IOS XE Release 3.4S	This command was modified. The *k6* argument was added.
15.2(2)T	This command was modified. The *k6* argument was added.
15.1(1)SY	This command was modified. The *k6* argument was added.

Usage Guidelines

Use this command to alter the default behavior of EIGRP routing and metric computation and to allow the tuning of the EIGRP metric calculation for a particular type of service (ToS).

If k5 equals 0, the composite EIGRP metric is computed according to the following formula:

metric = [k1 * bandwidth + (k2 * bandwidth)/(256 – load) + k3 * delay + K6 * extended metrics]

If k5 does not equal zero, an additional operation is performed:

metric = metric * [k5/(reliability + k4)]

Scaled Bandwidth= 10^7/minimum interface bandwidth (in kilobits per second) * 256

Delay is in tens of microseconds for classic mode and pico seconds for named mode. In classic mode, a delay of hexadecimal FFFFFFFF (decimal 4294967295) indicates that the network is unreachable. In named mode, a delay of hexadecimal FFFFFFFFFFFF (decimal 281474976710655) indicates that the network is unreachable.

Reliability is given as a fraction of 255. That is, 255 is 100 percent reliability or a perfectly stable link.

Load is given as a fraction of 255. A load of 255 indicates a completely saturated link.

Examples

The following example shows how to set the metric weights to slightly different values than the defaults:

```
Router(config)# router eigrp 109
Router(config-router)# network 192.168.0.0
Router(config-router)# metric weights 0 2 0 2 0 0
```

The following example shows how to configure an address-family metric weight to ToS: 0; K1: 2; K2: 0; K3: 2; K4: 0; K5: 0; K6:1:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4533
Router(config-router-af)# metric weights 0 2 0 2 0 0 1
```

Related Commands

Command	Description
address-family (EIGRP)	Enters address family configuration mode to configure an EIGRP routing instance.
bandwidth (interface)	Sets a bandwidth value for an interface.
delay (interface)	Sets a delay value for an interface.
ipv6 router eigrp	Configures an IPv6 EIGRP routing process.
metric holddown	Keeps new EIGRP routing information from being used for a certain period of time.
metric maximum-hops	Causes IP routing software to advertise routes with a hop count higher than what is specified by the command (EIGRP only) as unreachable routes.
router eigrp	Configures an EIGRP routing process.

neighbor (EIGRP)

To define a neighboring device with which an Enhanced Interior Gateway Routing Protocol (EIGRP) device can exchange routing information, 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* [**lisp-encap** [*lisp-id*]]]

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 or subinterface through which peering sessions are established.
interface-number	Number of the interface or subinterface.
remote	(Optional) Specifies that the neighbor is remote.
maximum-hops	(Optional) Maximum hop count. Valid range is from 2 to 100. This argument is available only when the **remote** keyword is configured.
lisp-encap	(Optional) Specifies that any data to routes from this remote neighbor is Location/ID Separation Protocol (LISP) encapsulated.
lisp-top-id	(Optional) Identity of the LISP instance. Only one LISP ID is allowed per device.

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.

Release	Modification
12.4(6)T	This command was modified. 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.
Cisco IOS XE Release 3.10	This command was modified. The **lisp-encap** keyword an *lisp-id* argument were added.
15.3(3)S	This command was integrated into Cisco IOS Release 15.3(3)S.

Usage Guidelines

Multiple neighbor statements can be used to establish peering sessions with specific EIGRP neighbors. The interface through which EIGRP exchanges 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 shows how to configure EIGRP peering sessions with neighbors 192.168.1.1 and 192.168.2.2:

```
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 shows how to configure 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 ethernet 0/0
Router(config-router-af)# neighbor 10.1.1.2 loopback 0 remote 10
```

The following example shows how to enable EIGRP to identify and reach EIGRP Route Reflectors in a network. An EIGRP Route Reflector is an EIGRP peer that forms adjacencies with customer edge routers in a network and exchange routes between them without changing the next hop or metrics of these routes.

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# neighbor 192.168.1.1 gigabitethernet 0/0/1 remote 2 lisp-encap 1
```

Related Commands

Command	Description
address-family (EIGRP)	Enters address family configuration mode to configure an EIGRP routing instance.
ipv6 router eigrp	Creates and configures an EIGRP routing process in IPv6 configurations.
passive-interface	Disables sending routing updates on an interface.
router eigrp	Configures an EIGRP routing process.
network (EIGRP)	Specifies the network for an EIGRP routing process.

neighbor description

To associate a description with a neighbor, use the **neighbor description** command in router configuration mode or address family configuration mode. To remove the description, use the **no** form of this command.

neighbor {*ip-address*| *peer-group-name*} **description** *text*

no neighbor {*ip-address*| *peer-group-name*} **description** [*text*]

Syntax Description

ip-address	IP address of the neighbor.
peer-group-name	Name of an EIGRP peer group. This argument is not available in address-family configuration mode.
text	Text (up to 80 characters in length) that describes the neighbor.

Command Default

There is no description of the neighbor.

Command Modes

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

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	This command was modified. Address-family configuration mode was added.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Examples

In the following examples, the description of the neighbor is “peer with example.com”:

```
Router(config)# router bgp 109
Router(config-router)# network 172.16.0.0
Router(config-router)# neighbor 172.16.2.3 description peer with example.com
```

In the following example, the description of the address family neighbor is “address-family-peer”:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)#
network 172.16.0.0
Router(config-router-af)#
neighbor 172.16.2.3 description address-family-peer
```

Related Commands

Command	Description
address-family (EIGRP)	Enters address family configuration mode to configure an EIGRP routing instance.
network (EIGRP)	Specifies the network for an EIGRP routing process.
router eigrp	Configures the EIGRP address family process.

neighbor maximum-prefix (EIGRP)

To limit the number of prefixes that are accepted from a single Enhanced Interior Gateway Protocol (EIGRP) neighbor or from all EIGRP neighbors, use the **neighbor maximum-prefix** command in address family configuration mode. To disable this function, use the **no** form of this command.

Single Neighbor Configuration

neighbor *ip-address* **maximum-prefix** *maximum* [*threshold*] **[warning-only]**

no neighbor *ip-address* **maximum-prefix**

All Neighbor Configuration

neighbor maximum-prefix *maximum* [*threshold*] [{**[dampened]** [**reset-time** *minutes*] [**restart** *minutes*] [**restart-count** *number*]| **warning-only**}]

no neighbor maximum-prefix

Syntax Description

ip-address	IP address of a single peer.
maximum	Maximum number of prefixes accepted. The range for this argument is a number from 1 to 4294967295. **Note** The number of prefixes that can be configured is limited only by the available system resources on the router.
threshold	(Optional) Configures the router to generate syslog warning messages when the specified percentage of the maximum-prefix limit has been reached. The prefix percentage number that can be configured for the *threshold* argument is from 1 to 100. The default is 75 percent.
warning-only	(Optional) Configures the router to generate syslog messages only when the *maximum-prefix limit*is reached, instead of terminating the peering session. This keyword is disabled by default.
dampened	(Optional) Configures a decay penalty to be applied to the restart-time period each time the maximum-prefix limit is reached. The half-life for the decay penalty is 150 percent of the default or user-defined restart-time value in minutes. This keyword is disabled by default.

reset-time minutes	(Optional) Configures the router to reset the restart count to 0 after the default or configured reset-time period has expired. The value for the *minutes* argument is from 1 to 65535 minutes. The default reset-time period is 15 minutes.
restart minutes	(Optional) Configures a time period in which the router will not form adjacencies or accept redistributed routes from the RIB after the maximum-prefix limit has been reached. The value for the minutes argument is from 1 to 65535 minutes. The default restart-time period is 5 minutes.
restart-count *number*	(Optional) Configures the number of times a peering session can be automatically reestablished after the peering session has been torn down or after a redistribute route has been cleared and relearned because the maximum-prefix limit has been reached. The default restart-count limit is 3. **Caution** Once the restart count threshold has been crossed, you will need to enter the **clear ip route *** or **clear ip eigrp neighbor** command to reestablish normal peering and/or redistribution.

Command Default

The number of prefixes that can be configured is limited only by the available system resources on the router.

Command Modes

Address family configuration (config-router-af)

Command History

Release	Modification
12.0(29)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

The **neighbor maximum-prefix** command can be configured to protect an individual peering session or to protect all peering sessions. When this feature is enabled and the maximum-prefix limit has been reached, the router will tear down the peering session, clear all routes that were learned from the peer, and then place the peer in a penalty state for the default or user-defined time period. After the penalty time period expires, normal peering will be reestablished.

Note In EIGRP, **neighbor** commands have been traditionally used to configure static neighbors. In the context of the EIGRP Prefix Limiting feature, however, the **neighbor maximum-prefix** command can be used to configure the maximum-prefix limit for both statically configured neighbors and dynamically discovered neighbors.

When you configure the **neighbor maximum-prefix** command to protect a single peering session, only the maximum-prefix limit, the percentage threshold, and the warning-only configuration options can be configured. Session dampening, restart, and reset timers are configured on a global basis.

Inherited Timer Values

Default or user-defined restart, restart-count, and reset-time values for the process-level configuration of this feature, configured with the **maximum-prefix** command, are inherited by the **redistribute maximum-prefix** and **neighbor maximum-prefix** command configurations by default. If a single peer is configured with the **neighbor maximum-prefix** command, a process-level configuration or a configuration that is applied to all neighbors will be inherited.

Examples

Examples

The following example, starting in global configuration mode, configures the maximum prefix limit for a single peer. The maximum limit is set to 1000 prefixes, and the warning threshold is set to 80 percent. When the maximum prefix limit is reached for the configured neighbor, adjacency with this neighbor will be brought down and all routes learned from it will be cleared. The neighbor will be placed in a penalty state for 4 minutes (user-defined penalty value). This function will not affect the relationship with any other neighbor.

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# neighbor 10.0.0.1 maximum-prefix 1000 80

Router(config-router-af)# end
```

Examples

The following example, starting in global configuration mode, configures the maximum prefix limit for all peers. The maximum limit is set to 10,000 prefixes, the warning threshold is set to 90 percent, the restart timer is set to 4 minutes, a decay penalty is configured for the restart timer with the dampened keyword, and all timers are configured to be reset to 0 every 60 minutes. When the maximum prefix limit is reached for any neighbor, adjacency with this neighbor will be brought down and all routes learned from it will be cleared. This function will not affect the relationship with any other neighbor. The offending peer will be placed in a penalty state for 4 minutes (user-defined penalty value). A dampening exponential decay penalty will also be applied.

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 virtual-name autonomous-system 4453
Router(config-router-af)# neighbor maximum-prefix 10000 90 dampened reset-time 60 restart
4
Router(config-router-af)# end
```

Related Commands

Command	Description
address-family (EIGRP)	Enters address family configuration mode to configure an EIGRP routing instance.
clear ip eigrp neighbors	Deletes entries from the EIGRP neighbor table.
clear ip eigrp vrf neighbor	Deletes neighbor entries from the VRF table.
clear ip route	Deletes routes from the IP routing table.
neighbor maximum-prefix	Limits the number of prefixes that are accepted from a single EIGRP neighbor or from all EIGRP neighbors.
redistribute maximum-prefix (EIGRP)	Limits the number of prefixes redistributed into an EIGRP process.

network (EIGRP)

To specify the network for an Enhanced Interior Gateway Routing Protocol (EIGRP) routing process, use the **network** command in router configuration mode or address-family configuration mode. To remove an entry, use the **no** form of this command.

network *ip-address* [*wildcard-mask*]

no network *ip-address* [*wildcard-mask*]

Syntax Description

ip-address	IP address of the directly connected network.
wildcard-mask	(Optional) EIGRP wildcard bits. Wildcard mask indicates a subnetwork, bitwise complement of the subnet mask.

Command Default

No networks are specified.

Command Modes

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

Command History

Release	Modification
10.0	This command was introduced.
12.0(4)T	The *network-mask* argument was added.
12.0(22)S	Address-family support for EIGRP was added.
12.2(15)T	Address-family support for EIGRP was added.
12.2(18)S	Address-family support for EIGRP was added.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
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.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

When the **network** command is configured for an EIGRP routing process, the router matches one or more local interfaces. The **network** command matches only local interfaces that are configured with addresses that are within the same subnet as the address that has been configured with the **network**command. The router then establishes neighbors through the matched interfaces. There is no limit to the number of network statements **(network** commands) that can be configured on a router.

Use a wildcard mask as a shortcut to group networks together. A wildcard mask matches everything in the network part of an IP address with a zero. Wildcard masks target a specific host/IP address, entire network, subnet, or even a range of IP addresses.

When entered in address-family configuration mode, this command applies only to named EIGRP IPv4 configurations. Named IPv6 and Service Advertisement Framework (SAF) configurations do not support this command in address-family configuration mode.

Examples

The following example configures EIGRP autonomous system 1 and establishes neighbors through network 172.16.0.0 and 192.168.0.0:

```
Router(config)# router eigrp 1

Router(config-router)# network 172.16.0.0
Router(config-router)# network 192.168.0.0
Router(config-router)# network 192.168.0.0 255.255.255.0
```

The following example configures EIGRP address-family autonomous system 4453 and establishes neighbors through network 172.16.0.0 and 192.168.0.0:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# network 172.16.0.0
Router(config-router-af)# network 192.168.0.0
```

Related Commands

Command	Description
address-family (EIGRP)	Enters address-family configuration mode to configure an EIGRP routing instance.
router eigrp	Configures the EIGRP address-family process.

next-hop-self

To enable the Enhanced Interior Gateway Routing Protocol (EIGRP) to advertise routes with the local outbound interface address as the next hop, use the **next-hop-self** command in address family interface configuration mode. To instruct an EIGRP device to use the received next hop instead of the local outbound interface address, use the **no** form of this command.

next-hop-self

no next-hop-self[**no-ecmp-mode**]

Syntax Description

no-ecmp-mode	(Optional) Evaluates all paths to a network before advertising the paths out of an interface.

Command Default

The next-hop-self state is enabled by default, which allows EIGRP to use a local address in the next-hop field of its routing advertisements.

Command Modes

Address family interface (config-router-af-interface)

Command History

Release	Modification
15.0(1)M	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
Cisco IOS XE Release 3.5S	This command was modified. The **no-ecmp-mode** keyword was added.
15.2(1)S	This command was integrated into Cisco IOS Release 15.2(1)S. The **no-ecmp-mode** keyword was added.
15.2(3)T	This command was modified. The **no-ecmp-mode** keyword was added.

Usage Guidelines

The **next-hop-self** command is an interface-based command. EIGRP, by default, sets the next-hop value to the local outbound interface address for routes that it is advertising, even when advertising those routes back out of the same interface on which they were learned. To change this default, you must use the **no next-hop-self** command to instruct EIGRP to use the received next-hop value when advertising these routes.

The **no-ecmp-mode** option is an enhancement to the **no next-hop-self** command. When this option is enabled, all paths to a network in the EIGRP table are evaluated to check whether routes advertised from an interface were learned on the same interface. If the route advertised by an interface was learned on the same interface, the **no next-hop-self** configuration is honored and the received next hop is used to advertise this route. Disabling the next-hop self functionality is primarily useful in Dynamic Multipoint VPN (DMVPN) spoke-to-spoke topologies.

Before configuring the **no next-hop-self** command, you must disable the split-horizon functionality. Split horizon is a protocol-independent parameter that blocks route information from being advertised by a device out of any interface from which that information originated. Use the **no split-horizon** command to disable split horizon.

Examples

The following example shows how to change the default next-hop value in IPv4 address family interface configurations by disabling the next-hop self functionality and configuring EIGRP to use the received next-hop value to advertise routes:

```
Device(config)# router eigrp virtual-name
Device(config-router)# address-family ipv4 autonomous-system 33
Device(config-router-af)# af-interface ethernet0/0
Device(config-router-af-interface)# no next-hop-self no-ecmp-mode
```

The following example shows how to change the default next-hop value in IPv6 address family interface configurations:

```
Device(config)# router eigrp virtual-name
Device(config-router)# address-family ipv6 autonomous-system 33
Device(config-router-af)# af-interface ethernet0/0
Device(config-router-af-interface)# no next-hop-self no-ecmp-mode
```

Related Commands

Command	Description
address-family	Configures an EIGRP routing instance in address family configuration mode.
router eigrp	Configures an EIGRP routing process.
split-horizon (EIGRP)	Enables EIGRP split horizon.

nsf (EIGRP)

To enable Cisco nonstop forwarding (NSF) operations for the Enhanced Interior Gateway Routing Protocol (EIGRP), use the **nsf** command in router configuration or address family configuration mode. To disable EIGRP NSF and to remove the EIGRP NSF configuration from the running-configuration file, use the **no** form of this command.

nsf

no nsf

Syntax Description

This command has no arguments or keywords.

Command Default

EIGRP NSF is disabled.

Command Modes

Router configuration (config-router)

Address family configuration (config-router-af)

Command History

Release	Modification
12.2(18)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
15.0(1)M	This command was modified. Support for Address family configuration mode was added.
12.2(33)SRE	This command was modified. Support for Address family configuration mode was added.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
Cisco IOS XE Release 3.6S	This command was modified. Support for IPv6 and IPv6 VPN Routing and Forwarding (VRF) was added.
15.2(2)S	This command was modified. Support for IPv6 and IPv6 VRF was added.

Usage Guidelines

The **nsf** command is used to enable or disable EIGRP NSF support on an NSF-capable router. NSF is supported only on platforms that support High Availability.

Examples

The following example shows how to disable NSF:

```
Device# configure terminal
Device(config)# router eigrp 101
Device(config-router)# no nsf
Device(config-router)# end
```

The following example shows how to enable EIGRP IPv6 NSF:

```
Device# configure terminal
Device(config)# router eigrp virtual-name-1
Device(config-router)# address-family ipv6 autonomous-system 10
Device(config-router-af)# nsf
Device(config-router-af)# end
```

Related Commands

Command	Description
debug eigrp address-family ipv6 notifications	Displays information about EIGRP address family IPv6 event notifications.
debug eigrp nsf	Displays notifications and information about NSF events for an EIGRP routing process.
debug ip eigrp notifications	Displays information and notifications for an EIGRP routing process.
show ip protocols	Displays the parameters and the current state of the active routing protocol process.
show ipv6 protocols	Displays the parameters and the current state of the active IPv6 routing protocol process.
timers graceful-restart purge-time	Sets the graceful-restart purge-time timer to determine how long an NSF-aware router that is running EIGRP must hold routes for an inactive peer.
timers nsf converge	Sets the maximum time that the restarting router must wait for the end-of-table notification from an NSF-capable or NSF-aware peer.
timers nsf signal	Sets the maximum time for the initial restart period.

offset-list (EIGRP)

To add an offset to incoming and outgoing metrics to routes learned via Enhanced Interior Gateway Routing Protocol (EIGRP), use the **offset-list** command in router configuration mode or address family topology configuration mode. To remove an offset list, use the **no** form of this command.

offset-list {*access-list-number*| *access-list-name*} {**in**| **out**} *offset* [*interface-type interface-number*]

no offset-list {*access-list-number*| *access-list-name*} {**in**| **out**} *offset* [*interface-type interface-number*]

Syntax Description

access-list-number | *access-list-name*	Standard access list number or name to be applied. Access list number 0 indicates all networks (networks, prefixes, or routes). If the *offset* value is 0, no action is taken.
in	Applies the access list to incoming metrics.
out	Applies the access list to outgoing metrics.
offset	Positive offset to be applied to metrics for networks matching the access list. If the offset is 0, no action is taken.
interface-type	(Optional) Interface type to which the offset list is applied.
interface-number	(Optional) Interface number to which the offset list is applied.

Command Default

No offset values are added to incoming or outgoing metrics to routes learned via EIGRP.

Command Modes

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

Command History

Release	Modification
10.0	This command was introduced.
10.3	The *interface-type* and *interface-number* arguments were added.
11.2	The *access-list-name* argument was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

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

Usage Guidelines

The offset value is added to the routing metric. An offset list with an interface type and interface number is considered extended and takes precedence over an offset list that is not extended. Therefore, if an entry passes the extended offset list and the normal offset list, the offset of the extended offset list is added to the metric.

Examples

In the following example, the router applies an offset of 10 to the delay component of the router only to access list 21:

```
Router(config-router)# offset-list 21 out 10
```

In the following example, the router applies an offset of 10 to routes learned from Ethernet interface 0:

```
Router(config-router)# offset-list 21 in 10 ethernet 0
```

In the following example, the router applies an offset of 10 to routes learned from Ethernet interface 0 in an EIGRP named configuration:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 1
Router(config-router-af)# topology base
Router(config-router-af-topology)# offset-list 21 in 10 ethernet0
```

passive-interface (EIGRP)

To suppress Enhanced Interior Gateway Routing Protocol (EIGRP) hello packets and routing updates on interfaces while still including the interface addresses in the topology database, use the **passive-interface** command in router configuration mode, address-family configuration mode, or address-family interface configuration mode. To reenable outgoing hello packets and 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) Configures all interfaces as passive.
interface-type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface-number	(Optional) Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.

Command Default

Hello packets and routing updates are sent and received on the interface.

Command Modes

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

Command History

Release	Modification
15.0(1)M	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.3(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

Use the **passive-interface**(EIGRP) command to select interfaces that will not form EIGRP neighbor adjacencies yet include the interface addresses in the EIGRP topology database. When the **passive-interface** (EIGRP)

command is configured, networks defined on the interface are added to the EIGRP topology database while routing updates and hello packets over the passive interfaces are suppressed.

The **default** keyword sets all interfaces to passive. Individual interfaces can be specified to override the default passive-interface state by using the **no passive-interface**command. The **default** keyword is useful when there are more passive interfaces than active interfaces. If the **default** keyword is not specified, the interfaces are considered nonpassive.

Examples

The following example shows how to place the router in the router configuration mode and set all EIGRP interfaces to the passive state and then set Ethernet interface 0/0 to a nonpassive state:

```
Router(config)# router eigrp 109
Router(config-router)# passive-interface default
Router(config-router)# no
 passive-interface ethernet0/0
```

The following example shows how to place the router in the address-family configuration mode and set all EIGRP interfaces in VRF RED to the passive state and then set Ethernet interface 0/0 to a nonpassive state:

```
Router(config)# router eigrp 109
Router(config-router)# address-family ipv4 vrf RED
Router(config-router-af)# passive-interface default
Router(config-router-af)# no passive-interface ethernet0/0
```

The following EIGRP named address-family interface configuration example sets all interfaces in an address family to passive and then sets Ethernet 0/0 to a nonpassive state:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# af-interface default
Router(config-router-af-interface)# passive-interface
Router(config-router-af-interface)# exit
Router(config-router-af)# af-interface ethernet0/0
Router(config-router-af-interface)# no passive-interface
```

Related Commands

Command	Description
address-family (EIGRP)	Enters address-family configuration mode to configure an EIGRP routing instance.
af-interface	Enters address-family interface configuration mode to configure interface-specific EIGRP commands.
network (EIGRP)	Specifies the network for an EIGRP routing process.
router eigrp	Configures the EIGRP address-family process.

redistribute eigrp

To redistribute IPv4 routes from Enhanced Interior Gateway Routing Protocol (EIGRP), use the **redistribute eigrp** command in router configuration mode. To disable the configuration, use the **no** form of this command.

redistribute eigrp *system-number* [**metric** *bandwidth-metric delay-metric reliability-metric effective-bandwidth-metric mtu-bytes*] [**route-map** *pointer-name*]

no redistribute eigrp *system-number* [**metric** *bandwidth-metric delay-metric reliability-metric effective-bandwidth-metric mtu-bytes*] [**route-map** *pointer-name*]

Syntax Description

system-number	Autonomous system number. The range is from 1 to 65535.
metric	(Optional) Specifies the metric for redistributed routes.
bandwidth-metric	(Optional) Maximum bandwidth of the route, in kilobits per second (kb/s). The range is from 1 to 4294967295.
delay-metric	(Optional) EIGRP route delay metric, in microseconds. The range is from 1 to 4294967295.
reliability-metric	(Optional) EIGRP reliability metric. The range is from 0 to 255. • An EIGRP metric of 255 signifies 100 percent reliability.
effective-bandwidth- metric	(Optional) Effective bandwidth of the route. The range is from 1 to 255. • Effective bandwidth of 255 denotes 100 percent load.
mtu-bytes	(Optional) The smallest allowed value for the maximum transmission unit (MTU), in bytes. The range is from 1 to 65535.
route-map	(Optional) Specifies the route map reference.
pointer-name	(Optional) Pointer to route-map entries.

Command Default

Route redistribution is disabled.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
12.2(8)T	This command was introduced in a release earlier than Cisco IOS Release 12.2(8)T.
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.
Cisco IOS XE Release 2.1	This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

Use the **redistribute eigrp** command to redistribute the routes learned through the EIGRP routing instances to other routing protocols. Forward redistribution of the EIGRP routes is allowed before creating the EIGRP routing instance. The EIGRP redistribution takes place as soon as the routing instance is created.

The metric value specified in the **redistribute**command supersedes the metric value specified using the **default-metric**command.

Note In Cisco IOS Release 12.0(33)S, the **redistribution eigrp**command is not allowed if the EIGRP router is not defined. The command terminates by displaying the following error message: %Configure eigrp router mode before redistributing

Examples

The following example shows how to configure a router to redistribute EIGRP routes into an EIGRP process:

```
Router# configure terminal

Router(config)# router eigrp virtual-name
Router(config-router)# redistribute eigrp 6473 metric 1 2 3 4 5
```

The following example shows the behavior of the **redistribution eigrp**command when the EIGRP router is not defined in Cisco IOS Release 12.0(33)S:

```
Router# configure terminal
Router(config)# router ospf 100 vrf vrf1
Router(config-router)# redistribute eigrp 99
%Configure eigrp router mode before redistributing
```

Related Commands

Command	Description
default-metric	Sets metrics for EIGRP.

redistribute maximum-prefix (EIGRP)

To limit the number of prefixes redistributed into an Enhanced Interior Gateway Routing Protocol (EIGRP) process, use the **redistribute maximum-prefix**command in address family configuration mode or address-family topology configuration mode. To disable this function, use the **no** form of this command.

redistribute maximum-prefix *maximum* [*threshold*] [**[dampened]** [**reset-time** *minutes*] [**restart** *minutes*] [**restart-count** *number*]| **[warning-only]**]

no redistribute maximum-prefix

Syntax Description

maximum	Maximum number of prefixes that are redistributed into EIGRP under an address family. The range for this argument is a number from 1 to 4294967295. **Note** The number of prefixes that can be configured is limited only by the available system resources on the router.
threshold	(Optional) The prefix percentage number. Valid values are 1 to 100. The default is 75. This value causes the router to generate syslog warning messages when the specified percentage of the maximum-prefix limit has been exceeded.
dampened	(Optional) Configures a decay penalty to be applied to the restart-time period each time the maximum-prefix limit is exceeded. The half-life for the decay penalty is 150 percent of the default or user-defined restart-time value in minutes. This keyword is disabled by default.
reset-time *minutes*	(Optional) Configures the router to reset the restart count to 0 after the default or configured reset-time period has expired. The value for the minutes argument is from 1 to 65535 minutes. The default reset-time period is 15 minutes.
restart *minutes*	(Optional) Configures a time period in which the router will not form adjacencies or accept redistributed routes from the Routing Information Base (RIB) after the maximum-prefix limit has been exceeded. The value for the *minutes* argument is from 1 to 65535 minutes. The default restart-time period is 5 minutes.

restart-count *number*	(Optional) Configures the number of times a peering session can be automatically be reestablished after the peering session has been torn down or after a redistribute route has been cleared and relearned because the maximum-prefix limit has been exceeded. The default restart-count limit is 3. **Caution** Once the restart count threshold has been crossed, you will need to enter the **clear ip route *** or **clear ip eigrp neighbor**command to reestablish normal peering and/or redistribution.
warning-only	(Optional) Configures the router to generate syslog messages only when the maximum-prefix limit is reached, instead of suspending redistribution. This keyword is disabled by default.

Command Default

The number of prefixes redistributed into an EIGRP process is not limited.

Command Modes

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

Command History

Release	Modification
12.0(29)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
15.0(1)M	This command was modified. Address family topology configuration mode was added.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

The **redistribute maximum-prefix** command is used to configure limit prefixes learned through redistribution. When the maximum-prefix limit is exceeded, all routes learned from the RIB will be discarded and redistribution will be suspended for the default or user-defined time period. The maximum-prefix limit that can be configured for redistributed prefixes is limited only by the available system resources on the router.

Inherited Timer Values

Default or user-defined restart, restart-count, and reset-time values for the process-level configuration of this feature, configured with the **maximum-prefix** command, are inherited by the redistribute **maximum-prefix** (EIGRP) and **neighbor maximum-prefix** (EIGRP) command configurations by default. If a single peer is

configured with the **neighbor maximum-prefix**(EIGRP) command, a process-level configuration or a configuration that is applied to all neighbors will be inherited.

Examples

The following example, starting in global configuration mode, configures the maximum prefix limit for routes learned through redistribution. The maximum limit is set to 5000 prefixes and the warning threshold is set to 95 percent. When the number of prefixes learned through redistribution reaches 4750 (95 percent of 5000), warning messages will be displayed in the console. Because the **warning-only** keyword was configured, the topology and routing tables will not be cleared and route redistribution will not be placed in a penalty state.

```
Router(config)# router eigrp 100
Router(config-router)# address-family ipv4 vrf RED
Router(config-router-af)# redistribute maximum-prefix 5000 95 warning-only
Router(config-router-af)# end
```

The following example shows this configuration in address-family topology configuration mode:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 vrf RED autonomous-system 4453
Router(config-router-af)# network 172.16.0.0
Router(config-router-af)# topology base
Router(config-router-af-topology)# redistribute maximum-prefix 5000 95 warning-only
Router(config-router-af-topology)# exit-af-topology
```

Related Commands

Command	Description
address-family (EIGRP)	Enters address-family configuration mode to configure an EIGRP routing instance.
clear ip eigrp neighbors	Deletes entries from the EIGRP neighbor table.
clear ip eigrp vrf neighbor	Deletes neighbor entries from the VRF table.
clear ip route	Deletes routes from the IP routing table.
network (EIGRP)	Specifies the network for an EIGRP routing process.
redistribute maximum-prefix (EIGRP)	Limits the number of prefixes redistributed into an EIGRP process.
topology (EIGRP)	Configures an EIGRP process to route IP traffic under the specified topology instance and enters address-family topology configuration mode.

remote-neighbors source (EIGRP)

To configure an Enhanced Interior Gateway Routing Protocol (EIGRP) process that enables remote neighbors to accept inbound connections from any remote IP address, use the **remote-neighbors source** command in address family configuration mode. To remove the configuration, use the **no** form of this command.

remote-neighbors source *interface-type interface-number* {**multicast-group** *group-address* | **unicast-listen lisp-encap** [*lisp-top-id*]}[**allow-list** *access-list-name*][**max-neighbor** *max-remote-peers*]

remote-neighbors source *interface-type interface-number* {**multicast-group** | **unicast-listen lisp-encap** [*lisp-top-id* | [**allow-list** *access-list-name*][**max-neighbor** *max-remote-peers*]]}

=

Syntax Description

interface-type interface-number	Interface to be used as the source for packets that are sent to remote neighbors.
multicast-group	Uses IP multicast to discover remote neighbors and form remote neighbor relationships.
group-address	Multicast address that EIGRP will use to discover remote neighbors and exchange information. Only devices using the same group address will discover one another as neighbors.
unicast-listen	Accepts connections initiated by remote neighbors and forms remote neighbor relationships without having to manually configure the remote neighbor IP address.
lisp-encap	Specifies that the data for this neighbor route will be Location/ID Separation Protocol (LISP) encapsulated.
lisp-top-id	(Optional) Identity of the LISP instance. Only one LISP ID is allowed per device.
allow-list	(Optional) Uses an Access Control List (ACL) to specify the remote IP addresses from which EIGRP neighbor connections may be accepted. If you do not use the **allow-list** keyword, then all IP addresses (permit any) will be accepted.
access-list-name	(Optional) Name of the ACL to be used with the **allow-list** keyword.
max-neighbors	(Optional) Uses the maximum number of remote neighbors. If you do not use this keyword, the maximum number of remote neighbors is limited only by the available memory and bandwidth.
max-remote-peers	(Optional) Maximum number of remote neighbors that a member of the multicast group may accept. The range is from 1 to 65535.

Command Default

No remote neighbors are specified.

Command Modes Address family configuration mode (config-router-af)

Command History

Release	Modification
Cisco IOS XE Release 3.10S	This command was introduced.
15.3(3)S	This command integrated into Cisco IOS Release 15.3(3)S.

Usage Guidelines You can use this command to configure EIGRP peers to receive unicast or multicast peering updates.

Examples The following example shows how to configure a customer edge router to receive unicast peering updates.

```
Device> enable
Device# configure terminal
Device(config)# router eigrp test
Device(config-router)# address family ipv4 unicast autonomous-system 100
Device(config-router-af)# remote-neighbors source gigabitEthernet 0/0/1 unicast-listen
lisp-encap 2
```

Related Commands

Command	Description
address-family (EIGRP)	Configures an EIGRP routing instance within an address family.
router EIGRP	Configures an EIGRP routing process.

router eigrp

To configure the Enhanced Interior Gateway Routing Protocol (EIGRP) routing process, use the **router eigrp** command in global configuration mode. To remove an EIGRP routing process, use the **no** form of this command.

router eigrp {*autonomous-system-number*| *virtual-instance-name*}

no router eigrp {*autonomous-system-number*| *virtual-instance-name*}

Syntax Description

autonomous-system-number	Autonomous system number that identifies the services to the other EIGRP address-family routers. It is also used to tag routing information. Valid range is 1 to 65535.
virtual-instance-name	EIGRP virtual instance name. This name must be unique among all address-family router processes on a single router, but need not be unique among routers.

Command Default

No EIGRP processes are configured.

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.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	This command was modified. The *virtual-instance-name* argument was added.
12.2(33)SRE	This command was modified. The *virtual-instance-name* argument was added.

Release	Modification
12.2(33)XNE	This command was modified. The *virtual-instance-name* argument was added.
Cisco IOS XE Release 2.5	This command was modified. The *virtual-instance-name* argument was added.

Usage Guidelines

Configuring the **router eigrp** command with the *autonomous-system-number*argument creates an EIGRP configuration referred to as autonomous system (AS) configuration. An EIGRP AS configuration creates an EIGRP routing instance that can be used for tagging routing information.

Configuring the **router eigrp** command with the *virtual-instance-name* argument creates an EIGRP configuration referred to as EIGRP named configuration. An EIGRP named configuration does not create an EIGRP routing instance by itself. An EIGRP named configuration is a base configuration that is required to define address-family configurations under it that are used for routing.

Examples

The following example configures EIGRP process 109:

```
Router(config)# router eigrp 109
```

The following example configures an EIGRP address-family routing process and assigns it the name “virtual-name”:

```
Router(config)#
router eigrp virtual-name
```

Related Commands

Command	Description
network (EIGRP)	Specifies a list of networks for the EIGRP process.

route-tag list

To create a route tag list, use the **route-tag list** command in global configuration mode. To remove the route tag list, use the **no** form of this command.

route-tag list *list-name* {**deny**| **permit**| **sequence** *number* {**deny**| **permit**}} *tag-value-dotted-decimal mask*

no route-tag list *list-name* [**sequence** *number* {**deny**| **permit**} *tag-value-dotted-decimal mask*]

Syntax Description

list-name	Name of the route tag list.
deny	Specifies packets that have to be rejected.
permit	Specifies packets that have to be forwarded.
sequence	Specifies the sequence number of an entry.
number	Sequence number. The valid range is from 1 to 4294967294.
tag-value-dotted-decimal	Route tag value in dotted-decimal format.
mask	Wildcard mask.

Command Default

No route tag list is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(2)S	This command was introduced.
Cisco IOS XE Release 3.6S	This command was integrated into Cisco IOS XE Release 3.6S.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.

Usage Guidelines

Use the **route-tag list** command to create route tag lists that will be used by route maps to match routes based on the criteria specified in the lists.

Examples

The following example shows how to configure a route tag list:

```
Device(config)# route-tag list list1 permit 1.1.1.1 0.0.0.1
Device(config)# route-tag list list1 sequence 5 permit 10.10.10.0 0.0.0.0
```

Related Commands

Command	Description
match tag list	Filters routes that match a specific route tag list.
route-tag notation	Enables the display of route tag values in dotted-decimal format.

route-tag notation

To enable the display of route tag values in dotted-decimal format, use the **route-tag notation** command in global configuration mode. To disable this functionality, use the **no** form of this command.

route-tag notation dotted-decimal

no route-tag notation dotted-decimal

Syntax Description

dotted-decimal	Enables the display of route tag values in dotted-decimal format.

Command Default

Tag values are displayed as plain decimals.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(2)S	This command was introduced.
Cisco IOS XE Release 3.6S	This command was integrated into Cisco IOS XE Release 3.6S.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.

Usage Guidelines

Configure the **route-tag notation** command to display route tag values in dotted-decimal format. When you configure this command, route tags are displayed as dotted decimals, irrespective of whether or not the route tags were configured as dotted decimals.

Examples

The following example shows how to configure the **route-tag notation** command:

```
Device(config)# route-tag notation dotted-decimal
```

Related Commands

Command	Description
eigrp default-route-tag	Sets a default route tag for all internal EIGRP routes.
match tag	Filters routes that match specified route tags.

Command	Description
set tag (IP)	Sets a tag value for routes.
show ip route	Displays contents of the IPv4 routing table.
show ipv6 route	Displays contents of the IPv6 routing table.
show route-map	Displays information about static and dynamic route maps.
show route-tag list	Displays information about route tag lists configured on the device.