IP Routing Protocol-Independent Commands: A through R

accept-ao-mismatch

Accepts segments even if there is a TCP-AO mismatch. For example a connection is still established in the following scenarios:

- The key-string or cryptographic algorithm do not match.
- The client is using a TCP-AO key, but the server is not using a TCP-AO key.

accept-ao-mismatch

Command Default

By default this option is disabled.

Command Modes

Key chain key configuration (config-keychain-key)

Command History

Release	Modification
16.12.1	This command was introduced.

Usage Guidelines

You must configure a key chain with keys to enable authentication.

Although you can identify multiple key chains, we recommend using one key chain per interface per routing protocol. Upon specifying the **key chain** command, you enter key chain configuration mode.

The following example configures a simple key chain for a TCP-AO enabled connection.

```
Router(config)# key chain kc1 tcp
Router(config-keychain)# key 7890
Router(config-keychain-key)# send-id 215
Router(config-keychain-key)# recv-id 215
Router(config-keychain-key)# key-string klomn
Router(config-keychain-key)# accept-ao-mismatch
```

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

accept-lifetime

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

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

Syntax Description

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

Command Default

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

Command Modes

Key chain key configuration (config-keychain-key)

Command History

Release	Modification
11.1	This command was introduced.
12.4(6)T	Support for IPv6 was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

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.

Usage Guidelines

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

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

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

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

Examples

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

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

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

```
Router(config)# router
 eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# network 10.0.0.0
Router(config-router-af)# af-interface ethernet0/0
Router(config-router-af-interface)# authentication key-chain trees
Router(config-router-af-interface)# authentication mode md5
Router(config-router-af-interface)# exit
Router(config-router-af)# exit
Router(config-router)# exit
Router(config)# key chain chain1
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string key1
Router(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 14:00:00 Jan 25 1996 duration 3600
Router(config-keychain-key)# exit
Router(config-keychain)# key 2
Router(config-keychain-key)# key-string key2
Router(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 15:00:00 Jan 25 1996 duration 3600
```

Related Commands

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

authentication (BFD)

To configure authentication in a Bidirectional Forwarding Detection (BFD) template for single hop and multihop sessions, use the **authentication** command in BFD configuration mode. To disable authentication in BFD template for single-hop and multihop sessions, use the **no** form of this command.

authentication *authentication-type* **keychain** *keychain-name*
no authentication *authentication-type* **keychain** *keychain-name*

Syntax Description

authentication-type	Authentication type. Valid values are md5, meticulous-md5, meticulous-sha-1, and sha-1.
keychain *keychain-name*	Configures an authentication key chain with the specified name. The maximum number of characters allowed in the name is 32.

Command Default

Authentication in BFD template for single hop and multihop sessions is not enabled.

Command Modes

BFD configuration (config-bfd)

Command History

Release	Modification
15.1(3)S	This command was introduced.
15.2(4)S	This command was modified. This command can be configured in both single hop and multihop templates.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.

Usage Guidelines

You can configure authentication in single hop and multihop templates. We recommend that you configure authentication to enhance security. Authentication must be configured on each BFD source-destination pair, and authentication parameters must match on both devices.

Examples

The following example shows how to configure authentication for the template1 BFD single-hop template:

```
Device> enable
Device# configuration terminal
Device(config)# bfd-template single-hop template1
Device(config-bfd)# authentication sha-1 keychain bfd-singlehop
```

The following example shows how to configure authentication for template1 BFD multihop template:

```
Device> enable
Device# configuration terminal
Device(config)# bfd-template multi-hop template1
Device(config-bfd)# authentication sha-1 keychain bfd-multihop
```

Related Commands

Command	Description
bfd	Sets the baseline BFD session parameters on an interface.
bfd map	Configures a BFD map that associates timers and authentication with multihop templates.
bfd-template	Configures a BFD template.

bfd

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

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

Syntax Description

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

Command Default

No baseline BFD session parameters are set.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)SXE	This command was introduced.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S.
12.2S	This command was modified. Support for IPv6 was added.
12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	This command was implemented on Cisco ASR 1000 Series Aggregation Services Routers.
12.2(33)SRE	This command was modified. Support for IPv6 was added.
15.0(1)M	This command was modified. Support was removed from ATM and inverse multiplexing over ATM (IMA) interfaces.
15.1(2)T	This command was modified. Support for IPv6 was added.
Cisco IOS XE Release 3.4	This command was modified. Support for point-to-point IPv4, IPv6, and generic routing encapsulation (GRE) tunnels was added.

Release	Modification
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
15.3(1)S	This command was modified. Support for multilink interface was added.
15.2(1)E	This command was integrated into Cisco IOS Release 15.2(1)E.

Usage Guidelines

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

- ATM
- Dot1Q VLAN subinterfaces (with an IP address on the Dot1Q subinterface)
- Ethernet
- Frame Relay
- Inverse Multiplexing over ATM (IMA)
- IP tunnel
- Port channel
- PoS
- Multilink
- Serial
- Tunnel (The tunnel type must be point-to-point, not Multiprotocol Label Switching (MPLS).

If BFD runs on a port channel interface, BFD has a timer value restriction of 750 * 3 milliseconds. Other interface types are not supported by BFD.

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

The bfd interval configuration is not removed when:

- an IPv4 address is removed from an interface
- an IPv6 address is removed from an interface
- IPv6 is disabled from an interface
- an interface is shutdown
- IPv4 CEF is disabled globally or locally on an interface
- IPv6 CEF is disabled globally or locally on an interface

The bfd interval configuration is removed when:

- the subinterface on which it is configured is removed

Examples

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

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

Related Commands

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

bfd all-interfaces

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

bfd all-interfaces
no bfd all-interfaces

Syntax Description

This command has no arguments or keywords.

Command Default

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

Command Modes

Router configuration (config-router)

Address family interface configuration (config-router-af)

Command History

Release	Modification
12.2(18)SXE	This command was introduced.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S.
12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS Release XE 2.1 and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.
12.2(33)SRE	This command was modified. Support for IPv6 was added.
15.0(1)M	This command was modified. The **bfd all-interfaces** command in named router configuration mode was replaced by the **bfd** command in address family interface mode.
15.1(2)T	This command was modified. Support for IPv6 was added.
Cisco IOS XE Release 3.3	This command was modified. Support for the Routing Information Protocol (RIP) was added.
15.2(4)S	This command was modified. Support for IPv6 was added.
Cisco IOS XE Release 3.7S	This command was modified. Support for IPv6 was added.

Usage Guidelines

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

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

bfd command in address family interface configuration mode to achieve the same functionality as that of the **bfd all-interfaces** command in router configuration mode.

Examples

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

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

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

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

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

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

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

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

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

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

The following example shows how to enable IPv6 BFD for all IS-IS neighbors, in address family interface configuration mode:

```
Router> enable
Router# configure terminal
Router(config)# router isis
Router(config-router)# address family ipv6
Router(config-router-af)# bfd all-interfaces
Router(config-router-af)# end
```

Related Commands

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

bfd check-ctrl-plane-failure

To enable Bidirectional Forwarding Detection (BFD) control plane failure checking for the Intermediate System-to-Intermediate System (IS-IS) routing protocol, use the **bfd check-control-plane-failure** command in router configuration mode. To disable control plane failure detection, use the **no** form of this command.

bfd check-ctrl-plane-failure
no bfd check-ctrl-plane-failure

Syntax Description

This command has no arguments or keywords.

Command Default

BFD control plane failure checking is disabled.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced.

Usage Guidelines

The **bfd check-ctrl-plane-failure** command can be configured for an IS-IS routing process only. The command is not supported on other protocols.

When a router restarts, a false BFD session failure can occur, where neighboring routers behave as if a true forwarding failure has occurred. However, if the **bfd check-ctrl-plane-failure** command is enabled on a router, the router can ignore control plane related BFD session failures. We recommend that you add this command to the configuration of all neighboring routers just prior to a planned router restart, and that you remove the command from all neighboring routers when the restart is complete.

Examples

The following example enables BFD control plane failure checking for the IS-IS routing protocol:

```
(config)# router isis
(config-router)# bfd check-ctrl-plane-failure
```

Related Commands

Command	Description
bfd	Sets the baseline BFD session parameters on an interface.
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process.

bfd echo

To enable Bidirectional Forwarding Detection (BFD) echo mode, use the **bfdecho** command in interface configuration mode. To disable BFD echo mode, use the **no** form of this command.

bfd echo
no bfd echo

Syntax Description

This command has no arguments or keywords.

Command Default

BFD echo mode is enabled by default.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	This command was modified. Support was removed from ATM and inverse multiplexing over ATM (IMA) interfaces.

Usage Guidelines

Echo mode is enabled by default. Entering the **nobfdecho** command without any keywords turns off the sending of echo packets and signifies that the router is unwilling to forward echo packets received from BFD neighbor routers.

When echo mode is enabled, the desired minimum echo transmit interval and required minimum transmit interval values are taken from the **bfdinterval***milliseconds***min_rx***milliseconds* parameters, respectively.

Note

If the **noiproute-cachesame-interface** command is configured, the **bfdechoaccept** command will not be accepted.

Note

Before using BFD echo mode, you must disable the sending of Internet Control Message Protocol (ICMP) redirect messages by entering the **noipredirects** command, in order to avoid high CPU utilization.

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

Echo Mode Without Asymmetry

Echo mode is described as without asymmetry when it is running on both sides (both BFD neighbors are running echo mode).

Examples

The following example configures echo mode between BFD neighbors:

```
Router> enable
Router# configure terminal
Router(config)# interface Ethernet 0/1
Router(config-if)# bfd
 echo
```

The following output from the **showbfdneighborsdetails** command shows that the BFD session neighbor is up and using BFD echo mode. The relevant command output is shown in bold in the output.

```
Router# show bfd neighbors details
OurAddr       NeighAddr      LD/RD  RH/RS    Holdown(mult)State    Int
172.16.1.2    172.16.1.1     1/6    Up       0    (3 )    Up       Fa0/1
Session state is UP and using echo function with 50 ms interval.
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3
Received MinRxInt: 1000000, Received Multiplier: 3
Holdown (hits): 3000(0), Hello (hits): 1000(337)
Rx Count: 341, Rx Interval (ms) min/max/avg: 1/1008/882 last: 364 ms ago
Tx Count: 339, Tx Interval (ms) min/max/avg: 1/1016/886 last: 632 ms ago
Registered protocols: EIGRP
Uptime: 00:05:00
Last packet: Version: 1            - Diagnostic: 0
             State bit: Up         - Demand bit: 0
             Poll bit: 0           - Final bit: 0
             Multiplier: 3         - Length: 24
             My Discr.: 6          - Your Discr.: 1
             Min tx interval: 1000000    - Min rx interval: 1000000
             Min Echo interval: 50000
```

Related Commands

Command	Description
bfd	Sets the baseline BFD session parameters on the interface.
ip redirects	Enables the sending of ICMP redirect messages if the Cisco IOS software is forced to resend a packet through the same interface on which it was received.
ip route-cache	Controls the use of switching methods for forwarding IP packets.

bfd interface

To enable Bidirectional Forwarding Detection (BFD) on a per-interface basis, use the **bfdinterface**command in router configuration mode. To disable BFD for all neighbors on a single interface, use the **no** form of this command.

bfd interface *type number*
no bfd interface *type number*

Syntax Description

type	Interface type for the interface to be enabled for BFD.
number	Interface number for the interface to be enabled for BFD.

Command Default

BFD is not enabled for the interface.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
12.2(18)SXE	This command was introduced.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S.
12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.0(1)M	This command was modified. The**bfdinterface** command in named router configuration mode was replaced by the**bfd**command in address family interface mode.

Usage Guidelines

In Cisco IOS Release 12.4(24)T and 12.2(33)SRA and earlier releases, the **bfdinterface** command works in router configuration mode and address-family intreface mode (af-interface mode).

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

Examples

The following example shows how to enable BFD for the Enhanced Interior Gateway Routing Protocol (EIGRP) neighbors on Fast Ethernet interface 3/0:

```
Router> enable
Router# configure terminal
Router(config)# router eigrp 123
Router(config-router)# bfd interface fastethernet 3/0
Router(config-if)# end
```

The following example shows how to enable the **bfd**command in address-family interface mode:

```
Router> enable
Router# configure terminal
```

```
Router(config)# router eigrp my_eigrp
Router(config-router)# address-family ipv4 autonomous-system 100

Router(config-router-af)# af-interface FastEthernet 0/0
Router(config-router-af-interface)# bfd
```

Related Commands

Command	Description
bfd	Sets the baseline BFD session parameters on an interface.
bfd all-interfaces	Enables BFD for all interfaces for a BFD peer.

bfd map

To configure a Bidirectional Forwarding Detection (BFD) map that associates timers and authentication with multihop templates, use the **bfd map** command in global configuration mode. To delete a BFD map, use the **no** form of this command.

bfd map {**ipv4** | **ipv6**} *destination* [**vrf** *vrf-name*] [{*source*}] *template-name*
no bfd map

Syntax Description

ipv4	Configures an IPv4 address.
ipv6	Configures an IPv6 address.
destination	The destination address.
vrf *vrf-name*	(Optional) Configures a VPN routing and forwarding instance (VRF).
source	(Optional) The source address.
template-name	The name of the template associated with the BFD map.

Command Default

If this command is not configured, a BFD map does not exist.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(3)S	This command was introduced.
15.2(2)SNG	This command was implemented on Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

The **show bfd neighbors** command can be used to help troubleshoot the BFD feature.

The full output for the **show bfd neighbors details** command is not supported on the Route Processor (RP) for the Cisco 12000 series Internet router. If you want to enter the **show bfd neighbors** command with the **details** keyword on the Cisco 12000 series Internet router, you must enter the command on the line card. Use the **attach** *slot* command to establish a CLI session with a line card.

In Cisco IOS Release 15.1(2)S and later releases that support BFD hardware offload, the Tx and Rx intervals on both BFD peers must be configured in multiples of 50 milliseconds. If they are not, output from the **show bfd neighbors details** command will show the configured intervals, not the changed ones.

For more information about prerequisites and restrictions for hardware offload, see the “Configuring Synchronous Ethernet on the Cisco 7600 Router with ES+ Line Card” section of the *Cisco 7600 Series Ethernet Services Plus (ES+) and Ethernet Services Plus T (ES+T) Line Card Configuration Guide*.

Cisco IOS Release 15.1(3)S and later releases support BFD on multiple network hops. The **bfd-template** command configures timers and authentication for a template. The **bfd map** command associates those timers and authentication with unique source/destination address pairs in multihop BFD sessions. Use the **bfd-template** command to configure a multihop template and the **bfd map** command to associate it with a map of destinations and associated BFD timers.

For IPv6 addresses, use X:X:X:X::X format; for IPv4 addresses, use the A.B.C.D. classless interdomain routing (CIDR) notation to represent the mask for both source and destination addresses.

Examples

The following example shows how to create a BFD multihop template, create a BFD map with IPv4 addresses, and associate the map with the template:

```
Router(config)# bfd-template multi-hop mh-template1
Router(bfd-config)# interval min-tx 200 min-rx 200 multiplier 3
Router(bfd-config)# authentication sha-1 keychain bfd_multihop
Router(bfd-config)# exit
Router(config)# bfd map ipv4 10.11.11.0/24 vrf vpn1 10.36.42.5/32 mh-template1
```

The following example shows how to create a BFD map with IPv6 addresses and associate it with a BFD multihop template:

```
Router(config)# bfd map ipv6 2001:DB8:0:1::/64 vrf v6_1 2001:DB8:0:2::/64 mh-template1
```

Related Commands

Command	Description
authentication	Configures authentication in BFD multihop sessions.
bfd	Set the baseline BFD session parameters on an interface.
bfd all-interfaces	Enables BFD for all router interfaces.
bfd echo	Enables BFD echo mode.
bfd interface	Enables BFD on a per-interface basis for a BFD peer.
bfd slow-timer	Configures the BFD slow timer value.
bfd-template	Configures a BFD template.
interval	Configures the transmit and receive intervals between BFD packets.
key chain	Configures an authentication key chain.

bfd slow-timers

To configure the Bidirectional Forwarding Detection (BFD) slow timers value, use the **bfdslow-timers** command in global configuration mode. This command does not have a **no** form.

bfd slow-timers [*milliseconds*]

Syntax Description

milliseconds	(Optional) BFD slow timers value, in milliseconds. The range is from 1000 to 30000. The default is 1000.

Command Default

The BFD slow timer value is 1000 milliseconds.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows how to configure the BFD slow timers value to 14,000 milliseconds:

```
Router(config)# bfd slow-timers 14000
```

The following output from the **showbfdneighborsdetails** command shows that the BFD slow timers value of 14,000 milliseconds has been implemented. The values for the MinTxInt and MinRxInt will correspond to the configured value for the BFD slow timers. The relevant command output is shown in bold.

```
Router# show bfd neighbors details
OurAddr        NeighAddr      LD/RD  RH/RS   Holdown(mult)  State     Int
172.16.10.1    172.16.10.2    1/1    Up      0    (3 )      Up        Et2/0
Session state is UP and using echo function with 50 ms interval.
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 14000, MinRxInt: 14000
, Multiplier: 3
Received MinRxInt: 10000, Received Multiplier: 3
Holdown (hits): 3600(0), Hello (hits): 1200(418)
Rx Count: 422, Rx Interval (ms) min/max/avg: 1/1480/1087 last: 112 ms ago
Tx Count: 420, Tx Interval (ms) min/max/avg: 1/2088/1090 last: 872 ms ago
Registered protocols: OSPF
Uptime: 00:07:37
Last packet: Version: 1            - Diagnostic: 0
             State bit: Up         - Demand bit: 0
             Poll bit: 0           - Final bit: 0
             Multiplier: 3         - Length: 24
             My Discr.: 1          - Your Discr.: 1
             Min tx interval: 14000 - Min rx interval: 14000
             Min Echo interval: 4000
```

Related Commands

Command	Description
bfd echo	Enables BFD echo mode.

bfd template

To bind a single hop Bidirectional Forwarding Detection (BFD) template to an interface, use the **bfd template** command in interface configuration mode. To unbind single-hop BFD template from an interface, use the **no** form of this command.

bfd template *template-name*
no bfd template *template-name*

Syntax Description

template-name	Name of the BFD template.

Command Default

A BFD template is not bound to an interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.2(4)S	This command was introduced.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.

Usage Guidelines

Even if you have not created the template by using the **bfd-template** command, you can configure the name of the template under an interface, but the template is considered invalid until you define the template. You do not have to reconfigure the template name again. It becomes valid automatically.

Examples

```
Device> enable
Device# configure terminal
Device(config)# interface Ethernet 0/1
Device(config-if)# bfd template template1
```

Related Commands

Command	Description
bfd-template	Creates a BFD template and enters BFD configuration mode.

bfd-template

To create a Bidirectional Forwarding Detection (BFD) template and to enter BFD configuration mode, use the **bfd-template** command in global configuration mode. To remove a BFD template, use the **no** form of this command.

bfd-template{**single-hop** | **multi-hop**} *template-name*
no bfd-template{**single-hop** | **multi-hop**} *template-name*

Syntax Description

single-hop	Creates the single-hop BFD template.
multi-hop	Creates the multihop BFD template.
template-name	Template name.

Command Default

A BFD template does not exist.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)S	This command was introduced.
15.1(3)S	This command was modified. The **multi-hop** keyword was added.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.

Usage Guidelines

The **bfd-template** command allows you to create a BFD template and places the device in BFD configuration mode. The template can be used to specify a set of BFD interval values. BFD interval values specified as part of the BFD template are not specific to a single interface.

The **bfd map** command associates timers and authentication in multihop templates with unique source/destination address pairs in multihop BFD sessions.

You can configure authentication in single-hop and multihop templates. Although it is not required, authentication is recommended to enhance security.

Examples

The following example shows how to create a BFD template and specify BFD interval values:

```
Device> enable
Device# configure terminal
Device(config)# bfd-template single-hop node1
Device(bfd-config)# interval min-tx 100 min-rx 100 multiplier 3
Device(bfd-config)# echo
```

The following example shows how to create a BFD single-hop template and configure BFD interval values and an authentication key chain:

```
Device> enable
Device# configure terminal
```

```
Device(config)# bfd-template single-hop template1
Device(bfd-config)# interval min-tx 200 min-rx 200 multiplier 3
Device(bfd-config)# authentication keyed-sha-1 keychain bfd_singlehop
```

The following example shows how to create a BFD multihop template and configure BFD interval values and an authentication key chain:

```
Device> enable
Device# configure terminal
Device(config)# bfd-template multi-hop template1
Device(bfd-config)# interval min-tx 200 min-rx 200 multiplier 3
Device(bfd-config)# authentication sha-1 keychain bfd-multihop
```

The following example shows how to change the type of an existing BFD template from single hop to multihop and vice versa:

```
Device> enable
Device# configure terminal
Device(config)# no bfd-template single-hop template1
Device(config)# bfd-template multi-hop template1
Device(bfd-config)# exit
Device(config)# no bfd-template multi-hop template1
Device(config)# bfd-template single-hop template1
```

Related Commands

Command	Description
authentication (BFD)	Configures authentication in BFD single-hop and multihop sessions.
bfd	Sets the baseline BFD session parameters on an interface.
bfd all-interfaces	Enables BFD for all router interfaces.
bfd echo	Enables BFD echo mode.
bfd interface	Enables BFD on a per-interface basis for a BFD peer.
bfd map	Configures a BFD map.
bfd slow-timer	Configures the BFD slow-timer value.
bfd template	Binds a single-hop BFD template to an interface.
echo	Enables BFD echo mode under a BFD template.
interval	Configures transmit and receive intervals between BFD packets.

cryptographic-algorithm

To specify the TCP cryptographic algorithm for a TCP-AO key, use the `cryptographic-algorithm` command in key chain key configuration mode.

cryptographic-algorithm *algorithm*

Syntax Description

algorithm	Specify one of the following authentication algorithms: • `aes-128-cmac`- AES-128-CMAC algorithm • `hmac-sha-1`- HMAC-SHA-1 algorithm • `hmac-sha-256`- HMAC-SHA-256 algorithm

Command Default

No algorithm is specified.

Command Modes

Key chain key configuration (config-keychain-key)

Command History

Release	Modification
16.12.1	This command was introduced.

Usage Guidelines

You must configure a key chain with keys to enable authentication.

Although you can identify multiple key chains, we recommend using one key chain per interface per routing protocol. Upon specifying the **key chain** command, you enter key chain configuration mode.

The following example configures a simple key chain for a TCP-AO enabled connection.

```
Router(config)# key chain kc1 tcp
Router(config-keychain)# key 7890
Router(config-keychain-key)# send-id 215
Router(config-keychain-key)# recv-id 215
Router(config-keychain-key)# key-string klomn
Router(config-keychain-key)# cryptographic-algorithm hmac-sha-1
```

Related Commands

Command	Description
key	Identifies an authentication key on a key chain.
key chain *key-name* **tcp**	Defines a TCP-AO authentication key-chain needed to enable authentication for routing protocols.
key-string (authentication)	Specifies the authentication string for a key.
show key chain	Displays authentication key information.

dampening

To configure a device to automatically dampen a flapping session, use the **dampening** command in interface configuration mode. To disable automatic dampening, use the **no** form of this command.

dampening [*half-life-period reuse-threshold suppress-threshold max-suppress-time*] [*restart-penalty*]
no dampening

Syntax Description

half-life-period	(optional) Time (in seconds) after which a penalty is decreased. Once the route has been assigned a penalty, the penalty is decreased by half after the half-life period expires. The range of the half-life period is from 1 to 30 seconds. The default time is 5 seconds.
reuse-threshold	(optional) Reuse value based on the number of penalties. When the accumulated penalty decreases enough to fall below this value, the route is unsuppressed. The range of the reuse value is from 1 to 20000; the default is 1000.
suppress-threshold	(optional) Value of the accumulated penalty that triggers the router to dampen a flapping interface. A route is suppressed when its penalty exceeds this limit. The range is from 1 to 20000; the default is 2000.
max-suppress-time	(optional) Maximum time (in seconds) a route can be suppressed. The range is from 1 to 20000; the default is four times the *half-life-periodvalue*. If the *half-life*-period value is allowed to default, the maximum suppress time defaults to 20 seconds.
restart-penalty	(optional) Penalty to applied to the interface when it comes up for the first time after the router reloads. The configurable range is from 1 to 18000 penalties. The default is 2000 penalties. This argument is not required for any other configurations.

Command Default

This command is disabled by default. To manually configure the timer for the restart-penalty argument, the value for all arguments must be manually entered.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

The IP Event Dampening feature will function on a subinterface but cannot be configured on only the subinterface. Only the primary interface can be configured with this feature. Primary interface configuration is applied to all subinterfaces by default.

When an interface is dampened, the interface is dampened to both IP and Connectionless Network Services (CLNS) routing equally. The interface is dampened to both IP and CLNS because integrated routing protocols such as Intermediate System-to-Intermediate System (IS-IS), IP, and CLNS routing protocols are closely interconnected, so it is impossible to apply dampening separately.

Copying a dampening configuration from virtual templates to virtual access interfaces is not supported because dampening has limited usefulness to existing applications using virtual templates. Virtual access interfaces are released when an interface flaps, and new connections and virtual access interfaces are acquired when the interface comes up and is made available to the network. Because dampening states are attached to the interface, the dampening states would not survive an interface flap.

If the **dampening**command is applied to an interface that already has dampening configured, all dampening states are reset and the accumulated penalty will be set to 0. If the interface has been dampened, the accumulated penalty will fall into the reuse threshold range, and the dampened interface will be made available to the network. The flap counts, however, are retained.

Examples

The following example sets the half life to 30 seconds, the reuse threshold to 1500, the suppress threshold to 10000, and the maximum suppress time to 120 seconds:

```
interface Ethernet 0/0
 dampening 30 1500 10000 120
```

The following example configures the router to apply a penalty of 500 on Ethernet interface 0/0 when the interface comes up for the first time after the router is reloaded:

```
interface Ethernet 0/0
 dampening 5 500 1000 20 500
```

Related Commands

Command	Description
clear counters	Clears the interface counters.
show dampening interface	Displays a summary of interface dampening.
show interface dampening	Displays a summary of the dampening parameters and status.

distance (IP)

To define an administrative distance for routes that are inserted into the routing table, use the **distance** command in router configuration mode. To return the administrative distance to its default distance definition, use the **no** form of this command.

distance *distance* *ip-address* *wildcard-mask* [{*ip-standard-aclaccess-list-name*}]
no **distance** *distance* *ip-address* *wildcard-mask* [{*ip-standard-aclaccess-list-name*}]

Syntax Description

distance	Administrative distance. An integer from 10 to 255. (The values 0 to 9 are reserved for internal use. Routes with a distance value of 255 are not installed in the routing table.)
ip-address	IP address in four-part, dotted decimal notation. The IP address or the network address from where routes are learned.
wildcard-mask	Wildcard mask in four-part, dotted decimal notation. A bit set to 1 in the *wildcard-mask* argument instructs the software to ignore the corresponding bit in the address value.
ip -standard-acl	(Optional) Standard IP access list (ACL) number to be applied to incoming routing updates.
access-list-name	(Optional) Named access list to be applied to incoming routing updates.

Command Default

For information on default administrative distances, see the “Usage Guidelines” section.

Command Modes

Router configuration(config-router)

Command History

Release	Modification
10.0	This command was introduced.
11.2	This command was modified. The *access-list-name*argument was added.
11.3	This command was modified. The ip keyword was removed.
12.0	This command was modified. The *ip-standard-acl*and*ip-extended-acl*arguments were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.0(1)M	This command was integrated into a release earlier than Cisco IOS Release 15.0(1)M.
15.2(4)S	This command was modified. The *ip-extended-acl* argument was removed.

Usage Guidelines

The table below lists default administrative distances.

Table 1: Default Administrative Distances

Route Source	Default Distance
Connected interface	0
Static route	1
Enhanced Interior Gateway Routing Protocol (EIGRP) summary route	5
External Border Gateway Protocol (eBGP)	20
Internal EIGRP	90
Open Shortest Path First (OSPF)	110
Intermediate System-to-Intermediate System (IS-IS)	115
Routing Information Protocol (RIP)	120
EIGRP external route	170
Internal BGP	200
Unknown	255

An administrative distance is a rating of the trustworthiness of a routing information source, such as an individual router or a group of routers. Numerically, an administrative distance is an integer from 0 to 255. In general, the higher the value, the lower the trust rating. An administrative distance of 255 means the routing information source cannot be trusted at all and should be ignored.

When the optional access list name is used with this command, it is applied when a network is being inserted into the routing table. This behavior allows filtering of networks according to the IP address of the router that supplies the routing information. This option could be used, for example, to filter possibly incorrect routing information from routers that are not under your administrative control.

Note Extended ACL is not supported for defining the administrative distance for a particular route which is inserted into the routing table. Use the standard IP access list to define the administrative distance.

The order in which you enter **distance** commands can affect the assigned administrative distances in unexpected ways. See the "Examples" section for further clarification.

For BGP, the **distance** command sets the administrative distance of the External BGP (eBGP) route.

For EIGRP, the **distance** command sets the administrative distance of only the internal routes of EIGRP neighbors. To set the administrative distance of external routes of EIGRP neighbors, use the **distance eigrp** command.

The **show ip protocols** privileged EXEC command displays the default administrative distance for the active routing processes.

Always set the administrative distance from the least to the most specific network.

Note The weight of a route can no longer be set with the distance command. To set the weight for a route, use a route map.

Examples

In the following example, the **router eigrp** global configuration command sets up EIGRP routing in autonomous system number 109. The **network** router configuration commands specify EIGRP routing on networks 192.168.7.0 and 172.16.0.0. The first **distance** command sets the administrative distance to 90 for all routers on the Class C network 192.168.7.0. The second **distance** command sets the administrative distance to 120 for the router with the address 172.16.1.3.

```
Device> enable
Device# configure terminal
Device(config)# router eigrp 109
Device(config-router)# network 192.168.7.0
Device(config-router)# network 172.16.0.0
Device(config-router)# distance 90 192.168.7.0 0.0.0.255
Device(config-router)# distance 120 172.16.1.3 0.0.0.255
Device(config-router)# end
```

In the following example, the set distance is from the least to the most specific network:

```
Device> enable
Device# configure terminal
Device(config)# router eigrp 109
Device(config-router)# distance 22 10.0.0.0 0.0.0.255
Device(config-router)# distance 33 10.11.0.0 0.0.0.255
Device(config-router)# distance 44 10.11.12.0 0.0.0.255
Device(config-router)# end
```

Note In this example, adding distance 255 to the end of the list would override the distance values for all networks within the range specified in the example. The result would be that the distance values are set to 255.

Entering the **show ip protocols** command displays the default administrative distance for the active routing processes, as well as the user-configured administrative distances:

```
Device# show ip protocols
.
.
.
Routing Protocol is "isis tag1"
  Invalid after 0 seconds, hold down 0, flushed after 0
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Redistributing: isis
  Address Summarization:
    None
  Maximum path: 4
  Routing for Networks:
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: (default is 115)
    Address         Wild mask       Distance  List
```

```
10.11.0.0            0.0.0.255       45
10.0.0.0             0.0.0.255       22
Address         Wild mask       Distance  List
10.11.0.0            0.0.0.255       33
10.11.12.0           0.0.0.255       44
```

Related Commands

Command	Description
distance (IPv6)	Configures an administrative distance for IS-IS, RIP, or OSPF IPv6 routes inserted into the IPv6 routing table.
distance (ISO CLNS)	Configures the administrative distance for CLNS routes learned.
distance bgp	Allows the use of external, internal, and local administrative distances that could be a better route to a node.
distance bgp (IPv6)	Allows the use of external, internal, and local administrative distances that could be a better route than other external, internal, or local routes to a node.
distance eigrp	Allows the use of two administrative distances--internal and external--that could be a better route to a node.
distance ospf	Defines OSPF route administrative distances based on route type.
show ip protocols	Displays the parameters and current state of the active routing protocol process.

distribute-list in (IP)

To filter networks received in updates, use the **distribute-list in** command in router configuration mode, address family configuration mode or address family topology configuration mode. To delete the distribution list and remove it from the running configuration file, use the **no** form of this command.

distribute-list {{*access-list-name* | *access-list-number* | **gateway** *prefix-list-name* | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*]} **in** [*interface-type interface-number*] | **route-map** *route-map-name* **in**}
no distribute-list {{*access-list-name* | *access-list-number* | **gateway** *prefix-list-name* | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*]} **in** [*interface-type interface-number*] | **route-map** *route-map-name* **in**}

Syntax Description

access-list-name	IP access-list name. The *access-list-name* argument defines which networks are to be received and which are to be suppressed in routing updates. • The range is from 1 to 199.
access-list-number	IP access-list number. The *access-list-number* argument defines which networks are to be received and which are to be suppressed in routing updates.
gateway	Filters incoming address updates based on a gateway.
prefix-list-name	IP prefix-list name. The *prefix-list-name* argument defines which routes from specified IP prefixes in the routing table are to be received and which are to be suppressed in routing updates.
prefix	Filters prefixes in address updates.
interface-type	(Optional) Type of interface. The *interface-type* argument defines the type of interface from which routing updates are to be received or suppressed. The *interface-type* argument cannot be used in address family configuration mode.
interface-number	(Optional) Interface number on which the access list should be applied to incoming updates. If no interface is specified, the access list will be applied to all incoming updates. The *interface-type* and *interface-number* arguments are applied if you specify an access list, not a route map. The *interface-number* argument cannot be used in address family configuration mode.
route-map	Specifies the route map that defines which networks are to be installed in the routing table and which are to be filtered from the routing table.
route-map-name	Name of route-map. The *route-map-name* argument defines the networks from which routing updates are to be received or suppressed. This argument is supported by OSPF, EIGRP and IS-IS.

Command Default

Networks received in updates are not filtered.

Command Modes

Router configuration (config-router)

Address family configuration (config-router-af)

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

Command History

Release	Modification
10.0	This command was introduced.
11.2	This command was modified. The *access-list-name*, *type*, and *number* arguments were added.
12.0(7)T	This command was modified. Address family configuration mode was added.
12.0(24)S	This command was modified. The **route-map** *route-map-name* keyword-argument pair was added.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was modified. Router address family topology configuration mode was added.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.3(3)M	This command was modified. The IS-IS protocol is now supported.

Usage Guidelines

The **distribute-list in** command is used to filter incoming updates. An access list, gateway, route map, or prefix list must be defined prior to configuration of this command. Standard and expanded access lists are supported. IP prefix lists are used to filter based on the bit length of the prefix. An entire network, subnet, supernet, or single host route can be specified. Prefix list and access list configuration is mutually exclusive when configuring a distribution list.

This command must specify either an access list or a map-tag name of a route map. The route map is supported for Open Shortest Path First (OSPF) and Enhanced Interior Gateway Routing Protocol (EIGRP) filtering.

The *interface-type* and *interface-number* arguments cannot be used in address family configuration mode.

OSPF routes cannot be filtered from entering the OSPF database. If you use this command for OSPF, it only filters routes from the routing table; it does not prevent link-state packets from being propagated.

If a route map is specified, the route map can be based on the following **match** options:

- **match interface**
- **match ip address**
- **match ip next-hop**
- **match ip route-source**
- **match metric**
- **match route-type**
- **match tag**

Configure the route map before specifying it in the **distribute-listin** command.

Release 12.2(33)SRB

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

Examples

In the following example, EIGRP process 1 is configured to accept two networks, network 0.0.0.0 and network 10.108.0.0:

```
Device(config)# access-list 1 permit 0.0.0.0
Device(config)# access-list 1 permit 10.108.0.0
Device(config)# access-list 1 deny 0.0.0.0 255.255.255.255
Device(config)# router eigrp 1
!
Device(config-router)# network 10.108.0.0
Device(config-router)# distribute-list 1 in
```

In the following EIGRP named configuration example, EIGRP is configured to accept two networks, network 0.0.0.0 and network 10.108.0.0:

```
Device(config)# access-list 1 permit 0.0.0.0
Device(config)# access-list 1 permit 10.108.0.0
Device(config)# access-list 1 deny 0.0.0.0 255.255.255.255
Device(config)# router eigrp virtual-name
!
Device(config-router)# address-family ipv4 autonomous-system 4453
Device(config-router-af)# network 10.108.0.0
Device(config-router-af)# network 10.0.0.0
Device(config-router-af)# topology base
Device(config-router-af-topology)# distribute-list 1 in
```

In the following EIGRP named configuration example, the address-family external route has a tag. The value of the tag is examined before the prefix is installed in the routing table. All address-family external addresses that have the tag value of 777 are filtered (prevented from being installed in the routing table). The permit statement with sequence number 20 has no match conditions, and there are no other route-map statements after sequence number 20, so all other conditions are permitted.

```
Device(config)# route-map tag-filter deny 10
Device(config-route-map)# match tag 777
Device(config-route-map)# route-map tag-filter permit 20
Device(config-route-map)# exit
Device(config)# router eigrp virtual-name
!
Device(config-router)# address-family ipv4 autonomous-system 4453
Device(config-router-af)# network 10.108.0.0
Device(config-router-af)# network 10.0.0.0
Device(config-router-af)# topology base
Device(config-router-af-topology)# distribute-list route-map tag-filter in
```

In the following example, OSPF external LSAs have a tag. The value of the tag is examined before the prefix is installed in the routing table. All OSPF external prefixes that have the tag value of 777 are filtered (prevented from being installed in the routing table). The permit statement with sequence number 20 has no match conditions, and there are no other route-map statements after sequence number 20, so all other conditions are permitted.

```
Device(config)# route-map tag-filter deny 10
Device(config-route-map)# match tag 777
Device(config-route-map)# route-map tag-filter permit 20
!
Device(config)# router ospf 1
Device(config-router)# router-id 10.0.0.2
Device(config-router)# log-adjacency-changes
Device(config-router)# network 172.16.2.1 0.0.0.255 area 0
Device(config-router)# distribute-list route-map tag-filter in
```

The following example shows how to filter three IS-IS routes from the routing table using a specified access list:

```
Device(config)# access-list 101 deny ip any 192.168.4.0 0.0.0.127
Device(config)# access-list 101 deny ip any 192.168.4.128 0.0.0.63
Device(config)# access-list 101 deny ip any 192.168.4.192 0.0.0.63
!
Device(config)# interface fastethernet 0/0
Device(config-if)# ip router isis 121
Device(config-if)# router isis 121
Device(config-router)# distribute-list 101 in
```

The following example shows how to filter three IS-IS routes from the routing table using a specified prefix list. Only a single command is required.

```
Device(config)# ip prefix-list List1 seq 3 deny 192.0.2.1/24
Device(config)# ip prefix-list List1 seq 5 deny 192.168.4.0/24 ge 25 le 26
Device(config)# ip prefix-list List1 seq 10 permit 0.0.0.0/le 32
!
Device(config)# interface fastethernet 0/0
Device(config-if)# ip router isis 122
Device(config-if)# router isis 122
Device(config-router)# distribute-list prefix List1 in
```

The following example shows how to filter IS-IS routes from the routing table using next hop:

```
Device(config)# ip prefix-list List2 seq 5 deny 198.51.100.31/24
!
Device(config)# interface fastethernet 0/0
Device(config-if)# ip router isis 125
Device(config-if)# router isis 125
Device(config-router)# distribute-list gateway List2 in
```

The following example shows how to filter IS-IS routes from the routing table using a specified route map:

```
Device(config)# route-map Map1 deny 10
Device(config-route-map)# match tag 200
Device(config-route-map)# exit
!
Device(config)# interface fastethernet 0/0
Device(config-if)# ip router isis 150
Device(config-if)# router isis 150
Device(config-router)# distribute-list route-map Map1 in
```

The following example shows how to enable IS-IS inbound filtering for routes that use standard IPv6 address prefixes:

```
Device(config)# ipv6 prefix-list 101 seq 5 deny 2001:DB8::/32
Device(config)# ipv6 prefix-list 102 seq 4 permit 2001:DB8::1/48 le 56
!
Device(config)# router isis
Device(config-router)# address-family ipv6
Device(config-router-af)# distribute-list prefix-list 101 in
Device(config-router-af)# distribute-list prefix-list 102 in ethernet 0/0
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
access-list (IP standard)	Defines a standard IP access list.
address-family ipv6	Configures routing sessions and enters address family configuration mode.
distribute-list out (IP)	Suppresses networks from being advertised in updates.
ip router isis	Configures an IS-IS routing process for IP on an interface and attaches an area designator to the routing process.
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.

distribute-list out (IP)

To suppress networks from being advertised in updates, use the **distribute-listout** command in the appropriate configuration mode.To cancel this function, use the **no** form of this command.

distribute-list {*access-list-numberaccess-list-name*} **out** [{*interface-namerouting-processas-number*}]
no distribute-list {*access-list-numberaccess-list-name*} **out** [{*interface-namerouting-processas-number*}]

Syntax Description

access-list-number | *access-list-name*	Standard IP access list number or name. The list defines which networks are to be sent and which are to be suppressed in routing updates.
interface-name	(Optional) Name of a particular interface. The *interface-name*argument cannot be used in address-family configuration mode.
routing-process	(Optional) Name of a particular routing process, or the **static** or **connected**keyword.
as-number	(Optional) Autonomous system number.

Command Default

This command is disabled by default. Networks are advertised in updates.

Command Modes

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

Command History

Release	Modification
10.0	This command was introduced.
11.2	The *access-list-name* argument was added.
12.0(7)T	Address family configuration mode was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	Address-family topology configuration mode was added.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When networks are redistributed, a routing process name can be specified as an optional trailing argument to the **distribute-list** command. Specifying this option causes the access list to be applied to only those routes derived from the specified routing process. After the process-specific access list is applied, any access list specified by a **distribute-list** command without a process name argument will be applied. Addresses not specified in the**distribute-list**command will not be advertised in outgoing routing updates.

The *interface-name*argument cannot be used in address-family configuration mode.

Note To filter networks that are received in updates, use the **distribute-listin** command.

Release 12.2(33)SRB

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

Examples

The following example would cause only one network to be advertised by a RIP routing process, network 10.108.0.0:

```
Router(config)# access-list 1 permit 10.108.0.0
Router(config)# access-list 1 deny 0.0.0.0 255.255.255.255
Router(config)# router rip
Router(config-router)# network 10.108.0.0
Router(config-router)# distribute-list 1 out
```

The following example applies access list 1 to outgoing routing updates. Only network 10.10.101.0 will be advertised in outgoing EIGRP routing updates.

```
Router(config)# router eigrp 100
Router(config-router)# distribute-list 1 out
Router(config-router)# exit
Router(config)# access-list 1 permit 10.10.101.0 0.0.0.255
```

The following EIGRP named configuration example applies access list 1 to outgoing routing updates and enables EIGRP address-family on Ethernet interface 0/0. Only network 10.0.0.0 will be advertised in outgoing EIGRP routing updates:

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

Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# network 10.10.0.0
Router(config-router-af)# topology base
Router(config-router-af-topology)# distribute-list 1 in
Router(config-router-af-topology)# exit-af-topology
Router(config-router-af-)# exit-address-family
Router(config-router)# exit
Router(config)# interface ethernet0/0
Router(config-if)# ip eigrp access-list 1 permit 10.10.101.0 0.0.0.255
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
access-list (IP standard)	Defines a standard IP access list.
address-family (EIGRP)	Enters address-family configuration mode to configure an EIGRP routing instance.
distribute-list in (IP)	Filters networks received in updates.
network (EIGRP)	Specifies the network for an EIGRP routing process.
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.
router eigrp	Configures the EIGRP address-family process.

Command	Description
topology (EIGRP)	Configures an EIGRP process to route IP traffic under the specified topology instance and enters router address-family topology configuration mode.

fast-reroute load-sharing disable

To disable Fast Reroute (FRR) load sharing of prefixes, use the **fast-reroute load-sharing disable** command in router configuration mode. To restore the default setting, use the **no** form of this command.

fast-reroute load-sharing {**level-1** | **level-2**} **disable**
no fast-reroute load-sharing {**level-1** | **level-2**} **disable**

Syntax Description

level-1	Specifies Level 1 packets.
level-2	Specifies Level 2 packets.

Command Default

Load sharing of prefixes is enabled by default.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
15.1(2)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.

Usage Guidelines

You must configure the **router isis** command before you can configure the **fast-reroute load-sharing disable** command.

Load sharing equally distributes the prefixes that use the same protected primary path over the available loop-free alternates (LFAs). An LFA is a next hop that helps a packet reach its destination without looping back.

Examples

The following example shows how to disable load sharing of Level 2 prefixes:

```
Router(config)# router isis
Router(router-config)# fast-reroute load-sharing level-2 disable
Router(router-config)# end
```

Related Commands

Command	Description
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process.

fast-reroute per-prefix

To enable Fast Reroute (FRR) per prefix, use the **fast-reroute per-prefix** command in router configuration mode. To disable the configuration, use the **no** form of this command.

fast-reroute per-prefix {**level-1** | **level-2**} {**all** | **route-map** *route-map-name*}
no fast-reroute per-prefix {**level-1** | **level-2**} {**all** | **route-map** *route-map-name*}

Syntax Description

level-1	Enables per-prefix FRR of Level 1 packets.
level-2	Enables per-prefix FRR of Level 2 packets.
all	Enables FRR of all primary paths.
route-map	Specifies the route map for selecting primary paths for protection.
route-map-name	Route map name.

Command Default

Fast Reroute per prefix is disabled.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
15.1(2)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)SNI	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

You must configure the **router isis** command before you can configure the **fast-reroute per-prefix** command.

You must configure the **all** keyword to protect all prefixes or configure the **route-map** *route-map-name* keyword and argument pair to protect a selected set of prefixes. When you specify the **all** keyword, all paths are protected, except paths that use interfaces, which are not supported, or interfaces, which are not enabled for protection. Using the **route-map** *route-map-name* keyword and argument pair to specify protected routes provides you with the flexibility to select protected routes, including using administrative tags.

Repair paths forward traffic during a routing transition. Repair paths are precomputed in anticipation of failures so that they can be activated when a failure is detected.

Examples

The following example shows how to enable FRR for all Level 2 prefixes:

```
Router(config)# router isis
Router(router-config)# fast-reroute per-prefix level-2 all
Router(router-config)# end
```

Related Commands

Command	Description
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process.

fast-reroute tie-break

To configure the Fast Reroute (FRR) tiebreaking priority, use the **fast-reroute tie-break** command in router configuration mode. To disable the configuration, use the **no** form of this command.

fast-reroute tie-break {**level-1** | **level-2**} {**downstream** | **linecard-disjoint** | **lowest-backup-path-metric** | **node-protecting** | **primary-path** | **secondary-path** | **srlg-disjoint**} *priority-number*
no fast-reroute tie-break {**level-1** | **level-2**} {**downstream** | **linecard-disjoint** | **lowest-backup-path-metric** | **node-protecting** | **primary-path** | **secondary-path** | **srlg-disjoint**}

Syntax Description

level-1	Configures tiebreaking for Level 1 packets.
level-2	Configures tiebreaking for Level 2 packets.
downstream	Configures loop-free alternates (LFAs) whose metric to the protected destination is lower than the metric of the protecting node to the destination.
linecard-disjoint	Configures LFAs that use interfaces that do not exist on the line card of the interface used by the primary path. The default is 40.
lowest-backup-path-metric	Configures LFAs with the lowest metric to the protected destination. The default is 30.
node-protecting	Configures LFAs that protect the primary next hop. The default is 50.
primary-path	Configures the repair path from the Equal Cost Multipath (ECMP) set. The default is 20.
secondary-path	Configures the non-ECMP repair path.
srlg-disjoint	Configures LFAs that do not share the same Shared Risk Link Group (SRLG) ID as the primary path. The default is 10.
priority-number	Priority number. Valid values are from 1 to 255.

Command Default

Tiebreaking is enabled by default.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
15.1(2)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.

Usage Guidelines

You must configure the **router isis** command before you can configure the **fast-reroute tie-break** command.

Tiebreaking configurations are applied per IS-IS instance per address family. The lower the configured priority value, the higher the priority of the rule. The same attribute cannot be configured more than once in the same address family.

The default tiebreaking rules have a priority value of 256. Hence, the tiebreaking rules that you configure will always have a higher priority than the default rule.

Load sharing equally distributes the prefixes that use the same protected primary path over the available LFAs. An LFA is a next hop that helps a packet reach its destination without looping back.

Examples

The following example shows how to set a tiebreaking priority of 5 for Level 2 packets:

```
Router(config)# router isis
Router(router-config)# fast-reroute tie-break level-1 downstream 150
Router(router-config)# end
```

Related Commands

Command	Description
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process.

echo

To enable Bidirectional Forwarding Detection (BFD) echo mode under a BFD template, use the **echo** command in BFD configuration mode. To disable BFD echo mode, use the **no** form of this command.

echo
no echo

Syntax Description

This command has no arguments or keywords.

Command Default

BFD echo mode is disabled.

Command Modes

BFD configuration (config-bfd)

Command History

Release	Modification
15.2(4)S	This command was introduced.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.

Usage Guidelines

Echo mode is disabled by default. Entering the **echo** command enables the sending of echo packets and signifies that the device is can forward echo packets received from BFD neighbor devices.

When echo mode is enabled, the desired minimum echo transmit interval and required minimum transmit interval values are derived from the values configured through the **interval** *milliseconds* **min-rx** *milliseconds* command.

Note If you configure the **no iproute-cache same-interface** command, the echo command is rejected.

Note Before using **echo** mode, you must disable the sending of Internet Control Message Protocol (ICMP) redirect messages by entering the **no ip redirects** command, in order to avoid high CPU utilization.

When echo mode is enabled on both BFD neighbors, the echo mode is described as without asymmetry.

Examples

The following example shows how to enable a BFD echo mode under a BFD template:

```
Device> enable
Device# configure terminal
Device(config)# bfd-template single-hop template1
Device(config-bfd)# echo
```

Related Commands

Command	Description
interval (BFD)	Configures the transmit and receive intervals between BFD packets.

Command	Description
ip redirects	Enables the sending of ICMP redirect messages if the Cisco software is forced to resend a packet through the same interface on which it was received.
ip route-cache	Controls the use of switching methods for forwarding IP packets.

include-tcp-options

indicates whether TCP options other than TCP-AO must be used to calculate MACs. With the flag enabled, the content of all options, in the order present, is included in the MAC and TCP-AO's MAC field is filled with zeroes. When the flag is disabled, all options other than TCP-AO are excluded from MAC calculations.

include-tcp-options

Command Default

This option is disabled.

Command Modes

Key chain key configuration (config-keychain-key)

Command History

Release	Modification
16.12.1	This command was introduced.

Usage Guidelines

This option must be configured on both devices.

You must configure a key chain with keys to enable authentication.

Although you can identify multiple key chains, we recommend using one key chain per interface per routing protocol. Upon specifying the **key chain** command, you enter key chain configuration mode.

The following example configures a simple key chain for a TCP-AO enabled connection. .

```
Router(config)# key chain kc1 tcp
Router(config-keychain)# key 7890
Router(config-keychain-key)# send-id 215
Router(config-keychain-key)# recv-id 215
Router(config-keychain-key)# key-string klomn
Router(config-keychain-key)# cryptographic-algorithm hmac-sha-1
Router(config-keychain-key)# include-tcp-options
```

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

interval (BFD)

To configure the transmit and receive intervals betweenBidirectional Forwarding Detection (BFD) packets, and to specify the number of consecutive BFD control packets that must be missed before BFD declares that a peer is unavailable, use the **interval**command in BFD configuration mode. To disable interval values use the **no** form of this command.

interval [**microseconds**]{**both** *milliseconds* | **min-tx** *milliseconds* **min-rx** *milliseconds*} [**multiplier** *multiplier-value*]
no interval

Syntax Description

microseconds	(Optional) Specifies the min-tx and min-rx timers in microseconds.
both *milliseconds*	Specifies the rate, in milliseconds, at which BFD control packets are sent to BFD peers and the rate at which BFD control packets are received from BFD peers. The valid range for the *milliseconds* argument is from 50 to 999.
min-tx *milliseconds*	Specifies the rate, in milliseconds, at which BFD control packets are sent to BFD peers. The valid range for the *milliseconds* argument is from 50 to 999.
min-rx *milliseconds*	Specifies the rate, in milliseconds, at which BFD control packets are received from BFD peers. The valid range for the *milliseconds* argument is from 50 to 999..
multiplier *multiplier-value*	(Optional) Specifies the number of consecutive BFD control packets that must be missed from a BFD peer before BFD declares that the peer is unavailable and the Layer 3 BFD peer is informed of the failure. The valid range is from 3 to 50. Default is 3.

Command Default

No session parameters are set.

Command Modes

BFD configuration (config-bfd)

Command History

Release	Modification
15.0(1)S	This command was introduced.
15.1(3)S	This command was modified. The **microseconds** keyword was added. ntroduced.
Cisco IOS XE 3.5S	This command was modified. Support for BDI interfaces was added.

Usage Guidelines

The **interval** command allows you to configure the session parameters for a BFD template.

Examples

The following example shows how to configure interval settings for the node1 BFD template:

```
Router(config)# bfd-template single-hop node1

Router(bfd-config)# interval min-tx 120 min-rx 100 multiplier 3
```

The following example shows how to configure interval settings for the template1 multihop BFD template:

```
Router(config)# bfd-template multi-hop template1

Router(bfd-config)# interval min-tx 200 min-rx 200 multiplier 3
```

Related Commands

Command	Description
authentication	Configures authentication in BFD multihop sessions.
bfd	Set the baseline BFD session parameters on an interface.
bfd all-interfaces	Enables BFD for all interfaces participating in the routing process.
bfd echo	Enables BFD echo mode.
bfd interface	Enables BFD on a per-interface basis for a BFD peer.
bfd slow-timer	Configures the BFD slow timer value.
bfd-template	Creates a BFD template and enters BFD configuration mode.

ip default-network

To select a network as a candidate route for computing the gateway of last resort, use the **ip default-network** command in global configuration mode. To remove a route, use the **no** form of this command.

ip default-network *network-number*
no ip default-network *network-number*

Syntax Description

network-number	Number of the network.

Command Default

If the router has a directly connected interface to the specified network, the dynamic routing protocols running on that router will generate (or source) a default route. For the Routing Information Protocol (RIP), this route flagged as the pseudo network 0.0.0.0.

Command Modes

Global configuration (config#)

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into Cisco IOS Release 12.2SX. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T.

Usage Guidelines

The Cisco IOS software uses both administrative distance and metric information to determine the default route. Multiple **ip default-network** commands can be used. All candidate default routes, both static (that is, flagged by the **ip default-network** command) and dynamic, appear in the routing table preceded by an asterisk.

If the IP routing table indicates that the specified network number is subnetted with a nonzero subnet number, the system will automatically configure a static summary route instead of a default route. The static summary route uses the specified subnet to route traffic destined for subnets that are not explicitly listed in the IP routing table to be routed.

The **ip default-network** command is a classful command. It is effective only if the network mask of the network that you wish to configure as a candidate route for computing the gateway of last resort matches the network mask in the Routing Information Base (RIB).

For example, if you configure **ip default-network 10.0.0.0** , then the mask considered by the routing protocol is 10.0.0.0/8, as it is a Class A network. The gateway of last resort is set only if the RIB contains a 10.0.0.0/8 route.

If you need to use the **ip default-network** command, ensure that the RIB contains a network route that matches the major mask of the network class.

Examples

The following example defines a static route to network 10.0.0.0 as the static default route:

```
ip route 10.0.0.0 255.0.0.0 10.108.3.4
ip default-network 10.0.0.0
```

If the following command is issued on a router that is not connected to network 10.140.0.0, the software might choose the path to that network as the default route when the network appears in the routing table:

```
ip default-network 10.140.0.0
```

Related Commands

Command	Description
show ip route	Displays the current state of the routing table.

ip gdp

To configure the router discovery mechanism, use the **ipgdp** command in global configuration mode. To disable the configuration, use the **no** form of this command.

ip gdp {**eigrp** | **irdp** [**multicast**] | **rip**}
no ip gdp {**eigrp** | **irdp** [**multicast**] | **rip**}

Syntax Description

eigrp	Configures a gateway to discover routers transmitting Enhanced Interior Gateway Routing Protocol (EIGRP) router updates.
irdp	Configures a gateway to discover routers transmitting ICMP Router Discovery Protocol (IRDP) router updates.
multicast	(Optional) Specifies the router to multicast IRDP solicitations.
rip	Configures a gateway to discover routers transmitting Routing Information Protocol (RIP) router updates.

Command Default

The router discovery mechanism is not configured.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

You must disable IP routing to configure the **ipgdp** command.

Examples

The following example shows how to configure the RIP router discovery mechanism:

```
Router# configure terminal
Router(config)# ip gdp rip
```

Related Commands

Command	Description
ip host	Defines static hostname-to-address mappings in the DNS hostname cache for a DNS view.
ip route	Establishes static routes.

ip local policy route-map

To identify a route map to use for local policy routing, use the **iplocalpolicyroute-map** command in global configuration mode. Todisable local policy routing, use the **no**form of this command.

ip local policy route-map commandip local policy route-map *map-tag*
no ip local policy route-map *map-tag*

Syntax Description

map-tag	Name of the route map to use for local policy routing. The name must match a *map-tag* value specified by a **route-map** command.

Command Default

Packets that are generated by the router are not policy routed.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Packets that are generated by the router are not normally policy routed. However, you can use this command to policy route such packets. You might enable local policy routing if you want packets originated at the router to take a route other than the obvious shortest path.

The **iplocalpolicyroute-map** command identifies a route map to use for local policy routing. Each **route-map** command has a list of **match**and **set** commands associated with it. The **match** commands specify the *matchcriteria*--the conditions under which packets should be policy routed. The **set** commands specify the *setactions*--the particular policy routing actions to perform if the criteria enforced by the **match** commands are met. The **noiplocalpolicyroute-map**command deletes the reference to the route map and disables local policy routing.

Examples

The following example sends packets with a destination IP address matching that allowed by extended access list 131 to the router at IP address 172.30.3.20:

```
ip local policy route-map xyz
!
route-map xyz
 match ip address 131
 set ip next-hop 172.30.3.20
```

Related Commands

Command	Description
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.

Command	Description
match length	Bases policy routing on the Level 3 length of a packet.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Indicates where to output packets that pass a match clause of route map for policy routing.
set ip default next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing and for which the Cisco IOS software has no explicit route to a destination.
set ip next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing.
show ip local policy	Displays the route map used for local policy routing.

ip policy route-map

To identify a route map to use for policy routing on an interface, use the **ip policy route-map** command in interface configuration mode. Todisable policy routing on the interface, use the **no**form of this command.

ip policy route-map *map-tag*
no ip policy route-map

Syntax Description

map-tag	Name of the route map to use for policy routing. The name must match a *map-tag* value specified by a **route-map** command.

Command Default

No policy routing occurs on the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.2	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You might enable policy routing if you want your packets to take a route other than the obvious shortest path.

The **ip policy route-map** command identifies a route map to use for policy routing. Each**route-map**command has a list of **match** and **set** commands associated with it. The **match** commands specify the *matchc riteria*--the conditions under which policy routing is allowed for the interface, based on the destination IP address of the packet. The **set** commands specify the *setactions*--the particular policy routing actions to perform if the criteria enforced by the **match** commands are met. The **no ip policy route-map** command deletes the pointer to the route map.

Policy routing can be performed on any match criteria that can be defined in an extended IP access list when using the**match ip address**command and referencing an extended IP access list.

The policy route map needs to reconfigured in an interface in the following scenarios:

- When a policy route map is applied to an interface with VRF configuration, the route map is removed and this information is sent to the CEF.
- When an interface is configured with a policy route map and VRF, the route map is removed whenever the VRF value changes.

Examples

The following example sends packets with the destination IP address of 172.21.16.18 to a router at IP address 172.30.3.20:

```
interface serial 0
```

```
 ip policy route-map wethersfield
!
route-map wethersfield
 match ip address 172.21.16.18
 set ip next-hop 172.30.3.20
```

Related Commands

Command	Description
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match length	Bases policy routing on the Level 3 length of a packet.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Indicates where to output packets that pass a match clause of route map for policy routing.
set ip default next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing and for which the Cisco IOS software has no explicit route to a destination.
set ip next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing.

ip route

To establish static routes, use the **iproute** command in global configuration mode. To remove static routes, use the **no**form of this command.

ip route [**vrf** *vrf-name*] *prefix* *mask* { *ip-address* | *interface-type* *interface-number* [*ip-address*] } [**dhcp**] [**global**] [*distance*] [**multicast**] [**name** *next-hop-name*] [{ **permanent** | **track** *number* }] [**tag** *tag*]
no **ip** **route** [**vrf** *vrf-name*] *prefix* *mask* { *ip-address* | *interface-type* *interface-number* [*ip-address*] } [**dhcp**] [**global**] [*distance*] **multicast** [**name** *next-hop-name*] [{ **permanent** | **track** *number* }] [**tag** *tag*]

To establish static routes, use the **ip route** command in global configuration mode. To remove static routes, use the **no** form of this command.

ip route *prefix mask* **segment-routing policy** [*policy name*]

no ip route

Syntax Description

vrf *vrf-name*	(Optional) Specifies name of the VRF for which static routes are configured.
prefix	IP route prefix for the destination.
mask	Prefix mask for the destination.
ip-address	IP address of the next hop that can be used to reach that network.
interface-type *interface-number*	Network interface type and interface number.
dhcp	(Optional) Enables a Dynamic Host Configuration Protocol (DHCP) server to assign a static route to a default gateway (option 3). **Note** Specify the **dhcp** keyword for each routing protocol.
global	(Optional) Specifies that the next hop address is global. **Note** This keyword is valid with the **vrf** *vrf-name* keyword and argument combination only and must be configured before any other keyword.
multicast	(Optional) Specifies that the static route being configured is a multicast route.
distance	(Optional) Administrative distance. The range is 1 to 255. The default administrative distance for a static route is 1.
name *next-hop-name*	(Optional) Applies a name to the next hop route.
permanent	(Optional) Specifies that the route will not be removed, even if the interface shuts down.
track *number*	(Optional) Associates a track object with this route. Valid values for the *number* argument range from 1 to 500.

tag *tag*	(Optional) Tag value that can be used as a “match” value for controlling redistribution via route maps.

Syntax Description

Syntax Description

prefix	IP route prefix for the destination.
mask	Prefix mask for the destination.
segment-routing policy	Configures the segment routing policy.
policy name	Name of the segment routing policy.

Command Default

No static routes are established.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.3(2)XE	The **track** keyword and *number* argument were added.
12.3(8)T	The **track** keyword and *number* argument were integrated into Cisco IOS Release 12.3(8)T. The **dhcp** keyword was added.
12.3(9)	The changes made in Cisco IOS Release 12.3(8)T were added to Cisco IOS Release 12.3(9).
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(1)T	This command was modified. The **dhcp** keyword was removed and the **global** keyword was added.
15.0(1)M	This command was modified. The **multicast** keyword was added.
Cisco IOS XE 17.3.1	Support for the keyword **segment-routing policy** [*policy name*] is introduced.

Usage Guidelines

The establishment of a static route is appropriate when the Cisco IOS software cannot dynamically build a route to the destination.

When you specify a DHCP server to assign a static route, the interface type and number and administrative distance may be configured also. In Cisco IOS Release 12.4(1)T and later releases, this keyword is removed.

For Cisco IOS Release 12.4(1)T and later releases, use the **global** keyword with the **vrf** *vrf-name* keyword and argument combination to specify that the next hop address is global.

If you specify an administrative distance, you are flagging a static route that can be overridden by dynamic information. For example, routes derived with Enhanced Interior Gateway Routing Protocol (EIGRP) have a default administrative distance of 100. To have a static route that would be overridden by an EIGRP dynamic route, specify an administrative distance greater than 100. Static routes have a default administrative distance of 1.

Static routes that point to an interface on a connected router will be advertised by way of Routing Information Protocol (RIP) and EIGRP regardless of whether **redistribute static** commands are specified for those routing protocols. This situation occurs because static routes that point to an interface are considered in the routing table to be connected and hence lose their static nature. Also, the target of the static route should be included in the **network** (DHCP) command. If this condition is not met, no dynamic routing protocol will advertise the route unless a **redistribute static**command is specified for these protocols. With the following configuration:

```
rtr1 (serial 172.16.188.1/30)--------------> rtr2(Fast Ethernet 172.31.1.1/30) ------>
router [rip | eigrp]
 network 172.16.188.0
 network 172.31.0.0
```

- RIP and EIGRP redistribute the route if the route is pointing to the Fast Ethernet interface:

```
ip route 172.16.188.252 255.255.255.252 FastEthernet 0/0
```

RIP and EIGRP do not redistribute the route with the following **ip route** command because of the split horizon algorithm:

```
ip route 172.16.188.252 255.255.255.252 serial 2/1
```

- EIGRP redistributes the route with both of the following commands:

```
ip route 172.16.188.252 255.255.255.252 FastEthernet 0/0
ip route 172.16.188.252 255.255.255.252 serial 2/1
```

With the Open Shortest Path First (OSPF) protocol, static routes that point to an interface are not advertised unless a **redistribute static** command is specified.

Adding a static route to an Ethernet or other broadcast interface (for example, ip route 0.0.0.0 0.0.0.0 Ethernet 1/2) will cause the route to be inserted into the routing table only when the interface is up. This configuration is not generally recommended. When the next hop of a static route points to an interface, the router considers each of the hosts within the range of the route to be directly connected through that interface, and therefore it will send Address Resolution Protocol (ARP) requests to any destination addresses that route through the static route.

A logical outgoing interface, for example, a tunnel, needs to be configured for a static route. If this outgoing interface is deleted from the configuration, the static route is removed from the configuration and hence does not show up in the routing table. To have the static route inserted into the routing table again, configure the outgoing interface once again and add the static route to this interface.

The practical implication of configuring the **ip route 0.0.0.0 0.0.0.0 ethernet 1/2** command is that the router will consider all of the destinations that the router does not know how to reach through some other route as directly connected to Ethernet interface 1/2. So the router will send an ARP request for each host for which it receives packets on this network segment. This configuration can cause high processor utilization and a large ARP cache (along with memory allocation failures). Configuring a default route or other static route that directs the router to forward packets for a large range of destinations to a connected broadcast network segment can cause your router to reload.

Specifying a numerical next hop that is on a directly connected interface will prevent the router from using proxy ARP. However, if the interface with the next hop goes down and the numerical next hop can be reached through a recursive route, you may specify both the next hop and interface (for example, ip route 0.0.0.0 0.0.0.0 ethernet 1/2 10.1.2.3) with a static route to prevent routes from passing through an unintended interface.

Note Configuring a default route that points to an interface, such as **ip route 0.0.0.0 0.0.0.0 ethernet 1/2**, displays the warning message: %Default routes, must specify a next hop IP address if not a point-to-point interface Router. This command causes the router to consider all the destinations that the router cannot reach through an alternate route, as directly connected to Ethernet interface 1/2. Hence, the router sends an ARP request for each host for which it receives packets on this network segment. This configuration can cause high processor utilization and a large ARP cache (along with memory allocation failures). Configuring a default route or other static route that directs the router to forward packets for a large range of destinations to a connected broadcast network segment can cause the router to reload.

The **name** *next-hop-name* keyword and argument combination allows you to associate static routes with names in your running configuration. If you have several static routes, you can specify names that describe the purpose of each static route in order to more easily identify each one.

The **track** *number* keyword and argument combination specifies that the static route will be installed only if the state of the configured track object is up.

Recursive Static Routing

In a recursive static route, only the next hop is specified. The output interface is derived from the next hop.

For the following recursive static route example, all destinations with the IP address prefix address prefix 192.168.1.1/32 are reachable via the host with address 10.0.0.2:

```
ip route 192.168.1.1 255.255.255.255 10.0.0.2
```

A recursive static route is valid (that is, it is a candidate for insertion in the IPv4 routing table) only when the specified next hop resolves, either directly or indirectly, to a valid IPv4 output interface, provided the route does not self-recurse, and the recursion depth does not exceed the maximum IPv4 forwarding recursion depth.

The following example defines a valid recursive IPv4 static route:

```
interface serial 2/0
 ip address 10.0.0.1 255.255.255.252
 exit
ip route 192.168.1.1 255.255.255.255 10.0.0.2
```

The following example defines an invalid recursive IPv4 static route. This static route will not be inserted into the IPv4 routing table because it is self-recursive. The next hop of the static route, 192.168.1.0/30, resolves via the first static route 192.168.1.0/24, which is itself a recursive route (that is, it only specifies a next hop). The next hop of the first route, 192.168.1.0/24, resolves via the directly connected route via the serial interface 2/0. Therefore, the first static route would be used to resolve its own next hop.

```
interface serial 2/0
 ip address 10.0.0.1 255.255.255.252
 exit
ip route 192.168.1.0 255.255.255.0 10.0.0.2
ip route 192.168.1.0 255.255.255.252 192.168.1.100
```

It is not normally useful to manually configure a self-recursive static route, although it is not prohibited. However, a recursive static route that has been inserted in the IPv4 routing table may become self-recursive as a result of some transient change in the network learned through a dynamic routing protocol. If this situation occurs, the fact that the static route has become self-recursive will be detected and the static route will be removed from the IPv4 routing table, although not from the configuration. A subsequent network change may cause the static route to no longer be self-recursive, in which case it will be re-inserted in the IPv4 routing table.

Note IPv4 recursive static routes are checked at one-minute intervals. Therefore, a recursive static route may take up to a minute to be inserted into the routing table once its next hop becomes valid. Likewise, it may take a minute or so for the route to disappear from the table if its next hop becomes invalid.

Examples

The following example shows how to choose an administrative distance of 110. In this case, packets for network 10.0.0.0 will be routed to a router at 172.31.3.4 if dynamic information with an administrative distance less than 110 is not available.

```
ip route 10.0.0.0 255.0.0.0 172.31.3.4 110
```

Note Specifying the next hop without specifying an interface when configuring a static route can cause traffic to pass through an unintended interface if the default interface goes down.

The following example shows how to route packets for network 172.31.0.0 to a router at 172.31.6.6:

```
ip route 172.31.0.0 255.255.0.0 172.31.6.6
```

The following example shows how to route packets for network 192.168.1.0 directly to the next hop at 10.1.2.3. If the interface goes down, this route is removed from the routing table and will not be restored unless the interface comes back up.

```
ip route 192.168.1.0 255.255.255.0 Ethernet 0 10.1.2.3
```

The following example shows how to install the static route only if the state of track object 123 is up:

```
ip route 0.0.0.0 0.0.0.0 Ethernet 0/1 10.1.1.242 track 123
```

The following example shows that using the **dhcp** keyword in a configuration of Ethernet interfaces 1 and 2 enables the interfaces to obtain the next-hop router IP addresses dynamically from a DHCP server:

```
ip route 10.165.200.225 255.255.255.255 ethernet1 dhcp
ip route 10.165.200.226 255.255.255.255 ethernet2 dhcp 20
```

The following example shows that using the **name** *next-hop-name* keyword and argument combination for each static route in the configuration helps you remember the purpose for each static route.

```
ip route 172.0.0.0 255.0.0.0 10.0.0.1 name Seattle2Detroit
```

The name for the static route will be displayed when the **show running-configuration** command is entered:

```
Router# show running-config
```

```
 | include ip route
ip route 172.0.0.0 255.0.0.0 10.0.0.1 name Seattle2Detroit
```

Examples

The following example shows how to configure static route traffic steering using SR-TE policy:

```
enable
configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#segment-routing mpls
Router(config-srmpls)# set-attributes
Router(config-srmpls-attr)# address-family ipv4
Router(config-srmpls-attr-af)# sr-label-preferred
Router(config-srmpls-attr-af)# explicit-null
Router(config-srmpls-attr-af)# exit-address-family
Router(config-srmpls-attr)# connected-prefix-sid-map
Router(config-srmpls-conn)# address-family ipv4
Router(config-srmpls-conn-af)# 1.1.1.1/32 index 1 range 1
Router(config-srmpls-conn-af)# exit-address-family
Router(config-srmpls-conn)#segment-routing traffic-eng
Router(config-srte)# segment-list name <segment-list name>
Router(config-srte-ep)# segment-list name <segment-list name>
Router(config-srte-ep)# index 1 mpls label 16005
Router(config-srte-ep)# index 2 mpls label 16010
Router(config-srte-ep)# index 3 mpls label 16009
Router(config-srte-ep)# policy <policy name>
Router(config-srte-policy)# color 50 end-point 21.21.21.21
Router(config-srte-policy)# candidate-paths
Router(config-srte-policy-path)# preference 100
Router(config-srte-policy-path-pref)# explicit segment-list <segment-list name>
Router(config-srte-policy-path-pref)# constraints
Router(config-srte-policy-path-pref-constr)# segments
Router(config-srte-policy-path-pref-constr-seg)# dataplane mpls
Router(config-srte-policy-path-pref-constr-seg)#end

Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip route 21.21.21.21 255.255.255.255 segment-routing policy <policy name>
```

Related Commands

Command	Description
network (DHCP)	Configures the subnet number and mask for a DHCP address pool on a Cisco IOS DHCP server.
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.

ip route profile

To enable IP routing table statistics collection, use the **iprouteprofile** command in global configuration mode. To disable collection of routing table statistics, use the **no** form of the command.

ip route profile commandp route profile
no ip route profile

Syntax Description

This command has no arguments or keywords.

Command Default

The time interval for each sample, or sampling interval, is a fixed value and is set at 5 seconds.

Command Modes

Global configuration

Command History

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

Usage Guidelines

The **iprouteprofile** command helps you to monitor routing table fluctuations that can occur as the result of route flapping, network failure, or network restoration.

This command identifies route flapping over brief time intervals. The time interval for each sample, or sampling interval, is a fixed value and is set at 5 seconds.

Two sets of statistics are collected. The per-interval statistics are collected over a sampling interval, while the routing table change statistics are the result of aggregating the per-interval statistics. The per-interval statistics are collected as a single set of counters, with one counter tracking one event. All counters are initialized at the beginning of each sampling interval; counters are incremented as corresponding events occur anywhere in the routing table.

At the end of a sampling interval, the per-interval statistics for that sampling interval are integrated with the routing table change statistics collected from the previous sampling intervals. The counters holding the per-interval statistics are reset and the process is repeated.

Routing table statistics are collected for the following events:

- Forward-Path Change. This statistic is the number of changes in the forwarding path, which is the accumulation of prefix-add, next-hop change, and pathcount change statistics.
- Prefix-Add. A new prefix was added to the routing table.
- Next-Hop Change. A prefix is not added or removed, but the next hop changes. This statistic is only seen with recursive routes that are installed in the routing table.
- Pathcount Change. The number of paths in the routing table has changed. This statistic is the result of an increase in the number of paths for an Interior Gateway Protocol (IGP) prefix in the routing table.
- Prefix Refresh. Standard routing table maintenance; the forwarding behavior is not changed.

Use the **showiprouteprofile** command to display the routing table change statistics.

Examples

The following example enables the collection of routing table statistics:

```
ip route profile
```

Related Commands

Command	Description
show ip route profile	Displays routing table change statistics.

ip route static adjust-time

To ch ange the time interval for IP static route adjustments during convergence, use the **iproutestaticadjust-time**command in global configuration mode. To reinstate the default adjustment time of 60 seconds, use the **no** form of this command.

ip route static adjust-time *seconds*
no ip route static adjust-time *seconds*

Syntax Description

seconds	Time of delay, in seconds, for convergence time during which the background process that monitors next-hop reachability is performed. The delay in convergence occurs when the route that covers the next hop is removed. The range is from 1 to 60. The default is 60.

Command Default

seconds : 60

Command Modes

Global configuration

Command History

Release	Modification
12.0(29)S	This command was introduced.
12.3(10)	This command was integrated into Cisco IOS Release 12.3(10).
12.3(11)T	This command was integrated into Cisco IOS Release 12.3(11)T.

Usage Guidelines

By default, static route adjustments are made every 60 seconds. To adjust the timer to any interval from 1 to 60 seconds, enter the ip route static adjust-time command.

The benefit of reducing the timer from the 60-second default value is to increase the convergence when static routes are used. However, reducing the interval can be CPU intensive if the value is set very low and a large number of static routes are configured.

Examples

In the following example, the adjustment time for static routes has been changed from the default 60 seconds to 30 seconds:

```
Router(config)# ip route static adjust-time 30
```

To remove the 30-second adjusted time interval and reinstate the default 60-second value, enter the **norouteipstaticadjust-time** command:

```
Router(config)# no ip route static adjust-time 30
```

Related Commands

Command	Description
show ip route	Displays the current state of the routing table.

ip route static bfd

To specify static route bidirectional forwarding detection (BFD) neighbors, use the **ip route static bfd** command in global configuration mode. To remove a static route BFD neighbor, use the **no** form of this command.

ip route static bfd {*interface-type interface-number ip-address* | **vrf** *vrf-name*} [*multihop-destination-address multihop-source-address*][**group** *group-name*] [{**passive**}] [{**unassociate**}]
no ip route static bfd {*interface-type interface-number ip-address* | **vrf** *vrf-name*} [*multihop-destination-address multihop-source-address*][**group** *group-name*] [{**passive**}] [{**unassociate**}]

Syntax Description

interface-type interface-number	Interface type and number.
ip-address	IP address of the gateway, in A.B.C.D format.
vrf *vrf-name*	Specifies Virtual Routing and Forwarding (VRF) instance and the destination vrf name.
multihop-destination-address multihop-source-address	Multihop destination and source address.
group *group-name*	(Optional) Assigns a BFD group. The group-name is a character string of up to 32 characters specifying the BFD group name.
unassociate	(Optional) Unassociates the static route configured for a BFD.

Command Default

No static route BFD neighbors are specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
15.1(2)S	This command was integrated into Cisco IOS Release 15.1(2)S. This command was modified. The **group** *group-name* keyword and argument pair and the **passive** keyword were added.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series.
Cisco IOS XE Release 3.8S	This command was integrated into a release prior to Cisco IOS XE Release 3.8S.
15.3(2)S	This command was modified. The **unassociate** keyword was added.

Usage Guidelines

Use the **ip route static bfd** command to specify static route BFD neighbors. All static routes that have the same interface and gateway specified in the configuration share the same BFD session for reachability notification.

All static routes that specify the same values for the *interface-type*, *interface-number*, and *ip-address* arguments will automatically use BFD to determine gateway reachability and take advantage of fast failure detection.

The *interface-type*, *interface-number*, and *ip-address* arguments are required because BFD supports only directly connected neighbors for the Cisco IOS 12.2(33)SRC,15.1(2)S and 15.1(2)SNG releases.

If the *interface-type*, *interface-number*, and *ip-address* arguments are used to configure a BFD session, it is a single hop BFD configuration. If **vrf**, *multihop-destination-address* or *multihop-source-address* arguments are used to configure a BFD session, it is a multihop BFD configuration.

The **group** keyword assigns a BFD group. The static BFD configuration is added to the VPN routing and forwarding (VRF) instance with which the interface is associated. The **passive** keyword specifies the passive member of the group. Adding static BFD in a group without the **passive** keyword makes the BFD an active member of the group. A static route should be tracked by the active BFD configuration in order to trigger a BFD session for the group. To remove all the static BFD configurations (active and passive) of a specific group, use the **no ip route static bfd** command and specify the BFD group name.

The **unassociate** keyword specifies that a BFD neighbor is not associated with static route, and the BFD sessions are requested if an interface has been configured with BFD. This is useful in bringing up a BFDv4 session in the absence of an IPv4 static route. If the **unassociate** keyword is not provided, then the IPv4 static routes are associated with BFD sessions.

BFD requires that BFD sessions are initiated on both endpoint devices. Therefore, this command must be configured on each endpoint device.

The BFD static session on a switch virtual interface (SVI) is established only after the **bfd interval** *milliseconds* **min_rx** *milliseconds* **multiplier** *multiplier-value* command is disabled and enabled on that SVI.

To enable the static BFD sessions, perform the following steps:

1. Enable BFD timers on the SVI.

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

2. Enable BFD for the static IP route

   ip route static bfd *interface-type interface-number ip-address*

3. Disable and enable the BFD timers on the SVI again.

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

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

Examples

The following example shows how to configure BFD for all static routes through a specified neighbor, group, and active member of the group:

```
Device# configure terminal
Device(config)# ip route static bfd GigabitEthernet 1/1 10.1.1.1 group group1
```

The following example shows how to configure BFD for all static routes through a specified neighbor, group, and passive member of the group:

```
Device# configure terminal
Device(config)# ip route static bfd GigabitEthernet 1/2 10.2.2.2 group group1 passive
```

The following example shows how to configure BFD for all static routes in an unassociated mode without the **group** and **passive** keywords:

```
Device# configure terminal
Device(config)#ip route static bfd GigabitEthernet 1/2 10.2.2.2 unassociate
```

Related Commands

Command	Description
bfd	Specifies the baseline BFD session parameters on an interface.
debug ip routing static bfd	Enables debugging output on IP static BFD neighbor events.
show ip static route bfd	Displays IPv4 static BFD configuration information from specific configured BFD groups and non-group entries.

ip route static install-routes-recurse-via-nexthop

To enable the installation of recursive static routes into the Routing Information Base (RIB), use the **ip route static install-routes-recurse-via-nexthop** command in global configuration mode. To remove this configuration, use the **no** form of this command.

ip route static install-routes-recurse-via-nexthop [{**all** | [{**multicast**}] [{**route-map** *map-name*}] [{**topology** *topology-name*}] [{**vrf** *vrf-name*}]}]
no ip route static install-routes-recurse-via-nexthop [{**all** | [{**multicast**}] [{**route-map** *map-name*}] [{**topology** *topology-name*}] [{**vrf** *vrf-name*}]}]

Syntax Description

all	(Optional) Installs all recursive static routes into the RIB.
multicast	(Optional) Installs recursive static routes into multicast topologies.
route-map *map-name*	(Optional) Installs recursive static routes defined by the specified route map into the RIB.
topology *topology-name*	(Optional) Installs recursive static routes into the specified topology.
vrf *vrf-name*	(Optional) Installs recursive static routes into the specified virtual routing and forwarding (VRF) instance.

Command Default

No recursive static routes are installed in the RIB.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.3(2)S	This command was introduced.
Cisco IOS XE Release 3.9S	This command was integrated into Cisco IOS XE Release 3.9S.
15.3(3)M	This command was integrated into Cisco IOS Release 15.3(3)M.

Usage Guidelines

Use the **ip route static install-routes-recurse-via-nexthop** command to install recursive static routes into the RIB. You can install recursive static routes in selected VRFs or topologies. You can use the **route-map** keyword to specify a route map for a specific VRF. The **multicast** keyword enables you to install recursive static routes in multicast topologies. If this command is used without any of the optional keywords, recursive static routes will be enabled only for the global VRF or topology. The **ip route static install-routes-recurse-via-nexthop** command is disabled by default.

Examples

The following example shows how to install recursive static routes into the RIB of a specific virtual routing and forwarding instance. This example is based on the assumption that a 10.0.0.0/8 route is already installed statically or dynamically in the RIB of vrf1.

```
Device> enable
Device# configure terminal
Device(config)# vrf definition vrf1
Device(config-vrf)# rd 1:100
Device(config-vrf)# address-family ipv4
Device(config-vrf-af)# exit
Device(config-vrf)# exit
Device(config)# ip route vrf vrf1 10.2.0.0 255.255.255.0 10.0.0.2
Device(config)# ip route static install-routes-recurse-via-nexthop vrf vrf1
Device(config)# end
```

Related Commands

Command	Description
address-family (VRF)	Specifies an address family type for a VRF instance.
ip route	Configures static routes to a network.
rd (IP)	Specifies a route distinguisher for a VRF instance.
vrf definition	Configures a VRF instance.

ip routing

To enable IP routing, use the **ip routing** command in global configuration mode. To disable IP routing, use the **no**form of this command.

ip routing
no ip routing

Syntax Description

This command has no arguments or keywords.

Command Default

IP routing is enabled.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

To bridge IP, the **no ip routing** command must be configured to disable IP routing. However, you need not specify **no ip routing** in conjunction with concurrent routing and bridging to bridge IP.

The ip routing command is disabled on the Cisco VG200 voice over IP gateway.

Disabling IP routing is not allowed if you are running Cisco IOS Release 12.2SX on a Catalyst 6000 platform. The workaround is to not assign an IP address to the SVI.

Examples

The following example enables IP routing:

```
Router# configure terminal
Router(config
)
# ip routing
```

ip routing protocol purge interface

To purge the routes of the routing protocols when an interface goes down, use the **iproutingprotocolpurgeinterface** command in global configuration mode. To disable the purging of the routes, use the **no** form of this command.

ip routing protocol purge interface
no ip routing protocol purge interface

Syntax Description

This command has no arguments or keywords.

Command Default

Routing protocols purge the routes by default when an interface goes down.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.0(27)SV	This command was integrated into Cisco IOS Release 12.0(27)SV.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.1(2)S	This command was modified. The command behavior was enabled by default.

Usage Guidelines

The **iproutingprotocolpurgeinterface** command allows the Routing Information Base (RIB) to ignore interface events for protocols that can respond to interface failures, thus eliminating any unnecessary deletion by the RIB. This in turn results in a single modify event to the Cisco Express Forwarding plane.

If the **noiproutingprotocolpurgeinterface** command is executed and a link goes down, the RIB process is automatically triggered to delete all prefixes that have the next hop on this interface from the RIB. The protocols on all the routers are notified, and if there is a secondary path, the protocols will update the RIB with the new path. When the process works through a large routing table, the process can consume many CPU cycles and increase the convergence time.

Examples

The following example shows how to disable the purge interface function for a routing protocol:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# no ip routing protocol purge interface
Router(config)# end
```

ipv6 local policy route-map

To enable local policy-based routing (PBR) for IPv6 packets, use the **ipv6 local policy route-map** command in global configuration mode. To disable local policy-based routing for IPv6 packets, use the **no** form of this command.

ipv6 local policy route-map *route-map-name*
no ipv6 local policy route-map *route-map-name*

Syntax Description

route-map-name	Name of the route map to be used for local IPv6 PBR. The name must match a *route-map-name* value specified by the **route-map** command.

Command Default

IPv6 packets are not policy routed.

Command Modes

Global configuration (config#)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)S.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Packets originating from a router are not normally policy routed. However, you can use the **ipv6 local policy route-map** command to policy route such packets. You might enable local PBR if you want packets originated at the router to take a route other than the obvious shortest path.

The **ipv6 local policy route-map** command identifies a route map to be used for local PBR. The **route-map** commands each have a list of **match** and **set** commands associated with them. The **match** commands specify the match criteria, which are the conditions under which packets should be policy routed. The **set** commands specify set actions, which are particular policy routing actions to be performed if the criteria enforced by the **match** commands are met. The **no ipv6 local policy route-map** command deletes the reference to the route map and disables local policy routing.

Examples

In the following example, packets with a destination IPv6 address matching that allowed by access list pbr-src-90 are sent to the router at IPv6 address 2001:DB8::1:

```
ipv6 access-list src-90
 permit ipv6 host 2001::90 2001:1000::/64
route-map pbr-src-90 permit 10
 match ipv6 address src-90
 set ipv6 next-hop 2001:DB8::1
ipv6 local policy route-map pbr-src-90
```

Related Commands

Command	Description
ipv6 policy route-map	Configures IPv6 PBR on an interface.
match ipv6 address	Specifies an IPv6 access list to be used to match packets for PBR for IPv6.
match length	Bases policy routing on the Level 3 length of a packet.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set default interface	Specifies the default interface to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Specifies the default interface to output packets that pass a match clause of a route map for policy routing.
set ipv6 default next-hop	Specifies an IPv6 default next hop to which matching packets will be forwarded.
set ipv6 next-hop (PBR)	Indicates where to output IPv6 packets that pass a match clause of a route map for policy routing.
set ipv6 precedence	Sets the precedence value in the IPv6 packet header.

ipv6 policy route-map

To configure IPv6 policy-based routing (PBR) on an interface, use the **ipv6 policy route-map** command in interface configuration mode. To disable IPv6 PBR on an interface, use the **no** form of this command.

ipv6 policy route-map *route-map-name*
no ipv6 policy route-map *route-map-name*

Syntax Description

route-map-name	Name of the route map to be used for PBR. The name must match the *map-tag* value specified by a **route-map** command.

Command Default

Policy-based routing does not occur on the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)S.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

You can enable PBR if you want your packets to take a route other than the obvious shortest path.

The **ipv6 policy route-map** command identifies a route map to be used for policy-based routing. The **route-map** commands each have a list of **match** and **set** commands associated with them. The **match** commands specify the match criteria, which are the conditions under which PBR is allowed for the interface. The **set** commands specify set actions, which are the PBR actions to be performed if the criteria enforced by the **match** commands are met. The **no ipv6 policy route-map** command deletes the pointer to the route map.

Policy-based routing can be performed on any match criteria that can be defined in an IPv6 access list.

Examples

In the following example, a route map named pbr-dest-1 is created and configured, specifying the packet match criteria and the desired policy-route action. Then, PBR is enabled on the interface Ethernet0/0.

```
ipv6 access-list match-dest-1
  permit ipv6 any 2001:DB8::1
route-map pbr-dest-1 permit 10
  match ipv6 address match-dest-1
  set interface Ethernet0/0
interface Ethernet0/0
  ipv6 policy-route-map pbr-dest-1
```

Related Commands

Command	Description
ipv6 local policy route-map	Identifies the route map to be used for local IPv6 PBR.
match ipv6 address	Specifies an IPv6 access list to be used to match IPv6 packets for PBR.
match length	Bases policy routing on the Level 3 length of a packet.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set default interface	Specifies the default interface to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Specifies the default interface to output packets that pass a match clause of a route map for policy routing.
set ipv6 default next-hop	Specifies an IPv6 default next hop to which matching packets will be forwarded.
set ipv6 next-hop	Specifies the default interface to output IPv6 packets that pass a match clause of a route map for policy routing.
set ipv6 precedence	Sets the precedence value in the IPv6 packet header.

ipv6 route static bfd

To specify static route Bidirectional Forwarding Detection for IPv6 (BFDv6) neighbors, use the **ipv6 route static bfd** command in global configuration mode. To remove a static route BFDv6 neighbor, use the **no** form of this command.

ipv6 route static bfd [**vrf** *vrf-name*] *interface-type interface-number ipv6-address* [**unassociated**]
no ipv6 route static bfd

Syntax Description

vrf *vrf-name*	(Optional) Name of the virtual routing and forwarding (VRF) instance by which static routes should be specified.
interface-type interface-number	Interface type and number.
ipv6-address	IPv6 address of the neighbor.
unassociated	(Optional) Moves a static BFD neighbor from associated mode to unassociated mode.

Command Default

No static route BFDv6 neighbors are specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.
15.1(2)T	This command was integrated into Cisco IOS Release 15.1(2)T.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
15.1(1)SY	This command was modified. Support for IPv6 was added to Cisco IOS Release 15.1(1)SY.
15.2(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

Use the **ipv6 route static bfd** command to specify static route neighbors. All of the static routes that have the same interface and gateway specified in the configuration share the same BFDv6 session for reachability notification. BFDv6 requires that BFDv6 sessions are initiated on both endpoint routers. Therefore, this command must be configured on each endpoint router. An IPv6 static BFDv6 neighbor must be fully specified (with the interface and the neighbor address) and must be directly attached.

All static routes that specify the same values for **vrf** *vrf-name*, *interface-type interface-number* , and *ipv6-address* will automatically use BFDv6 to determine gateway reachability and take advantage of fast failure detection.

Examples

The following example creates a neighbor on Ethernet interface 0/0 with an address of 2001::1:

```
Router(global config)# ipv6 route static bfd ethernet 0/0 2001::1
```

The following example converts the neighbor to unassociated mode:

```
Router(global config)# ipv6 route static bfd ethernet 0/0 2001::1 unassociated
```

Related Commands

Command	Description
show ipv6 static	Displays the current contents of the IPv6 routing table.

isdn supp-service callRerouteing

To enable ISDN partial rerouting on the BRI interface of Cisco 4000 Series Integrated Services Routers, use the **isdn supp-service callRerouteing** command in the interface configuration mode. To disable ISDN partial rerouting use the **no** form of the command.

isdn supp-service callRerouteing

Syntax Description

This command has no arguments or keywords.

Command Default

ISDN partial rerouting is not enabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
16.5.1	This command was introduced.

Usage Guidelines

This command is used when an ISDN destination phone has call diversion configured. This command enables the gateway to convert ISDN call reroute information (in ISDN facility messages based on ETS 300 207-1) from the destination into a SIP 302 message. As a result, the connection to the old destination is released and a new connection is established with the new destination. This feature is limited to the described call flow and is tested and supported with facility messages arriving from a particular Mitel PBX (IntelliGate 300) only.

ISDN partial rerouting can only be enabled on the bri-net3 switch type.

This feature is only supported if ISDN is used at the network side.

Example

The following example enables ISDN partial rerouting on interface bri1:

```
ISR4321-VoiceGW-LAB(config-if)#
ISR4321-VoiceGW-LAB(config-if)#int BRI0/1/0:0
ISR4321-VoiceGW-LAB(config-if)#isdn switch-type basic-net3
ISR4321-VoiceGW-LAB(config-if)#isdn protocol-emulate network
ISR4321-VoiceGW-LAB(config-if)#isdn supp-service callRerouteing
ISR4321-VoiceGW-LAB(config-if)#end
ISR4321-VoiceGW-LAB#
```

ipv6 route static resolve default

To allow a recursive IPv6 static route to resolve using the default IPv6 static route, use the **ipv6 route static resolve default**command in global configuration mode. To remove this function, use the **no** form of this command.

ipv6 route static resolve default
no ipv6 route static resolve default

Syntax Description

This command has no arguments or keywords.

Command Default

Recursive IPv6 static routes do not resolve via the default route.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)XNE	This command was introduced.

Usage Guidelines

By default, a recursive IPv6 static route will not resolve using the default route (::/0). The **ipv6 route static resolve default** command restores legacy behavior and allows resolution using the default route.

Examples

The following example enables an IPv6 recursive static route to be resolved using a IPv6 static default route:

```
Router(config)# ipv6 route static resolve default
```

key

To identify an authentication key on a key chain, use the **key** command in key-chain configuration mode. To remove the key from the key chain, use the **no** form of this command.

key *key-id*
no key *key-id*

Syntax Description

key-id	Identification number of an authentication key on a key chain. The range of keys is from 0 to 2147483647. The key identification numbers need not be consecutive.

Command Default

No key exists on the key chain.

Command Modes

Key-chain configuration (config-keychain)

Command History

Release	Modification
11.1	This command was introduced.
12.4(6)T	Support for IPv6 was added.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

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

It is useful to have multiple keys on a key chain so that the software can sequence through the keys as they become invalid after time, based on the **accept-lifetime** and **send-lifetime** key chain key command settings.

Each key has its own key identifier, which is stored locally. The combination of the key identifier and the interface associated with the message uniquely identifies the authentication algorithm and Message Digest 5 (MD5) authentication key in use. Only one authentication packet is sent, regardless of the number of valid keys. The software starts looking at the lowest key identifier number and uses the first valid key.

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

To remove all keys, remove the key chain by using the **no key chain** command.

Examples

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

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

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

```
Router(config)# router
eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# network 10.0.0.0
Router(config-router-af)# af-interface ethernet0/0
Router(config-router-af-interface)# authentication key-chain trees
Router(config-router-af-interface)# authentication mode md5
Router(config-router-af-interface)# exit
Router(config-router-af)# exit
Router(config-router)# exit
Router(config)# key chain chain1
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string key1
Router(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 14:00:00 Jan 25 1996 duration 3600
Router(config-keychain-key)# exit
Router(config-keychain)# key 2
Router(config-keychain-key)# key-string key2
Router(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 15:00:00 Jan 25 1996 duration 3600
```

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

```
Router(config)# eigrp virtual-name
Router(config-router)# service-family ipv4 autonomous-system 4453
Router(config-router-sf)# network 10.0.0.0
Router(config-router-sf)# sf-interface ethernet0/0
Router(config-router-sf-interface)# authentication key-chain trees
Router(config-router-sf-interface)# authentication mode md5
Router(config-router-sf-interface)# exit
Router(config-router-sf)# exit
Router(config-router)# exit
Router(config)# key chain chain1
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string key1
Router(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 14:00:00 Jan 25 1996 duration 3600
Router(config-keychain-key)# exit
Router(config-keychain)# key 2
Router(config-keychain-key)# key-string key2
Router(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 15:00:00 Jan 25 1996 duration 3600
```

Related Commands

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

key chain

To define an authentication key chain needed to enable authentication for routing protocols and enter key-chain configuration mode, use the **key chain** command in global configuration mode. To remove the key chain, use the **no** form of this command.

key chain chain *name-of-chain* **[tcp]**
no key chain *name-of-chain*

Syntax Description

name-of-chain	Name of a key chain. A key chain must have at least one key and can have up to 2147483647 keys.
tcp	Optionally sets the key chain to use the TCP Authentication Option (TCP-AO).

Command Default

No key chain exists.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.1	This command was introduced.
12.4(6)T	Support for IPv6 was added.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
16.12.1	Support for TCP-AO using the tcp option was added.

Usage Guidelines

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

You must configure a key chain with keys to enable authentication.

Although you can identify multiple key chains, we recommend using one key chain per interface per routing protocol. Upon specifying the **key chain** command, you enter key chain configuration mode.

Examples

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

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

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

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# network 10.0.0.0
Router(config-router-af)# af-interface ethernet0/0
Router(config-router-af-interface)# authentication key-chain trees
Router(config-router-af-interface)# authentication mode md5
Router(config-router-af-interface)# exit
Router(config-router-af)# exit
Router(config-router)# exit
Router(config)# key chain chain1
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string key1
Router(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 14:00:00 Jan 25 1996 duration 3600
Router(config-keychain-key)# exit
Router(config-keychain)# key 2
Router(config-keychain-key)# key-string key2
Router(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 15:00:00 Jan 25 1996 duration 3600
```

The following named configuration example configures a key chain named trees for service-family. The key named chestnut will be accepted from 1:30 pm to 3:30 pm and be sent from 2:00 pm to 3:00 pm. The key birch will be accepted from 2:30 pm to 4:30 pm and be sent from 3:00 pm to 4:00 pm. The overlap allows for migration of keys or a discrepancy in the set time of the router. There is a 30-minute leeway on each side to handle time differences.

```
Router(config)# router eigrp virtual-name
Router(config-router)# service-family ipv4 autonomous-system 4453
Router(config-router-sf)# sf-interface ethernet
Router(config-router-sf-interface)# authentication key chain trees
Router(config-router-sf-interface)# authentication mode md5
Router(config-router-sf-interface)# exit
Router(config-router-sf)# exit
Router(config-router)# exit
Router(config)# key chain chain1
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string chestnut
Router(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 14:00:00 Jan 25 1996 duration 3600
Router(config-keychain-key)# exit
Router(config-keychain)# key 2
Router(config-keychain-key)# key-string birch
Router(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 15:00:00 Jan 25 1996 duration 3600
```

The following example configures a simple key chain for a TCP-AO enabled connection. The key named tcpao1 will be accepted from 1:30 pm to 3:30 pm and be sent from 2:00 pm to 3:00 pm. The key tcpao2 will be accepted from 2:30 pm to 4:30 pm and be sent from 3:00 pm to 4:00 pm. The overlap allows for migration of keys or a discrepancy in the set time of the router. There is a 30-minute leeway on each side to handle time differences.

```
Router(config)# key chain kc1 tcp
Router(config-keychain)# key 1
Router(config-keychain-key)# send-id 215
Router(config-keychain-key)# recv-id 215
Router(config-keychain-key)# key-string tcpao1
Router(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 14:00:00 Jan 25 1996 duration 3600
Router(config-keychain-key)# cryptographic-algorithm hmac-sha-1
Router(config-keychain-key)# include-tcp-optionsRouter(config-keychain-key)# exit
outer(config-keychain)# key 2
Router(config-keychain-key)# send-id 215
Router(config-keychain-key)# recv-id 215
Router(config-keychain-key)# key-string tcpao2
Router(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 15:00:00 Jan 25 1996 duration 3600
Router(config-keychain-key)# cryptographic-algorithm hmac-sha-1
Router(config-keychain-key)# include-tcp-options
```

Related Commands

Command	Description
accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.
ip rip authentication key-chain	Enables authentication for RIP Version 2 packets and specifies the set of keys that can be used on an interface.
ip authentication key-chain eigrp	Enables authentication of EIGRP packets.
key	Identifies an authentication key on a key chain.
key-string (authentication)	Specifies the authentication string for a key.
send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.
show key chain	Displays authentication key information.

key-string (authentication)

To specify the authentication string for a key, use the **key-string**(authentication) command in key chain key configuration mode. To remove the authentication string, use the **no** form of this command.

key-string *text*
no key-string *text*

Syntax Description

text	Authentication string that must be sent and received in the packets using the routing protocol being authenticated. The string can contain from 1 to 80 uppercase and lowercase alphanumeric characters.

Command Default

No authentication string for a key exists.

Command Modes

Key chain key configuration (config-keychain-key)

Command History

Release	Modification
11.1	This command was introduced.
12.4(6)T	Support for IPv6 was added.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Only DRP Agent, Enhanced Interior Gateway Routing Protocol (EIGRP), and Routing Information Protocol (RIP) Version 2 use key chains. Each key can have only one key string.

If password encryption is configured (with the **service password-encryption** command), the software saves the key string as encrypted text. When you write to the terminal with the **more system:running-config** command, the software displays key-string 7 encrypted text.

Examples

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

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

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

```
Router(config)# eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# network 10.0.0.0
Router(config-router-af)# af-interface ethernet0/0
Router(config-router-af-interface)# authentication key-chain trees
Router(config-router-af-interface)# authentication mode md5
Router(config-router-af-interface)# exit
Router(config-router-af)# exit
Router(config-router)# exit
Router(config)# key chain chain1
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string key1
Router(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 14:00:00 Jan 25 1996 duration 3600
Router(config-keychain-key)# exit
Router(config-keychain)# key 2
Router(config-keychain-key)# key-string key2
Router(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 15:00:00 Jan 25 1996 duration 3600
```

Related Commands

Command	Description
accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.
ip authentication key-chain eigrp	Enables authentication of EIGRP packets.
key	Identifies an authentication key on a key chain.
key chain	Defines an authentication key-chain needed to enable authentication for routing protocols.
send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.
service password-encryption	Encrypts passwords.
show key chain	Displays authentication key information.

match interface (IP)

To distribute any routes that have their next hop out one of the interfaces specified, use the **matchinterface** command in route-map configuration mode. To remove the **matchinterface** entry, use the **no** form of this command.

match interface *interface-type interface-number* [. . . *interface-type interface-number*]
no match interface *interface-type interface-number* [. . . *interface-type interface-number*]

Syntax Description

interface- type	Interface type.
interface- number	Interface number.

Command Default

No match interfaces are defined.

Command Modes

Route-map configuration (config-route-map)

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.
15.1(2)S	This command was integrated into Cisco IOS Release 15.1(2)S.

Usage Guidelines

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *interface-typeinterface-number* arguments .

Use the **route-map** global configuration command, and the **match** and **set** route-map configuration commands, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *matchcriteria*--the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the *setactions*--the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **noroute-map** command deletes the route map.

The **match** route-map configuration command has multiple formats. The **match** commands may be given in any order, and all **match** commands must “pass” to cause the route to be redistributed according to the *setactions*given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

A route map can have several parts. Any route that does not match at least one **match** clause relating to a **route-map** command will be ignored; that is, the route will not be advertised for outbound route maps and will not be accepted for inbound route maps. If you want to modify only some data, you must configure a second route map section with an explicit match specified.

Examples

In the following example, routes that have their next hop out Ethernet interface 0 will be distributed:

```
route-map name
 match interface ethernet 0
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community	Matches a BGP community.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match ip next-hop	Redistributes any routes that have a next hop router address passed by one of the access lists specified.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match metric (IP)	Redistributes routes with the metric specified.
match route-type (IP)	Redistributes routes of the specified type.
match tag	Redistributes routes in the routing table that match the specified tags.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set as-path	Modifies an autonomous system path for BGP routes.
set automatic-tag	Automatically computes the tag value.
set community	Sets the BGP communities attribute.
set level (IP)	Indicates where to import routes.
set local-preference	Specifies a preference value for the autonomous system path.
set metric (BGP, OSPF, RIP)	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set next-hop	Specifies the address of the next hop.
set tag (IP)	Sets a tag value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.

match ip address

To distribute any routes that have a destination network number address that is permitted by a standard access list, an extended access list, or a prefix list, or to perform policy routing on packets, use the **matchipaddress** command in route-map configuration mode. To remove the **matchipaddress** entry, use the **no** form of this command.

match ip address {*access-list-number* [{*access-list-number* **. . .** | *access-list-name* **. . .**}] | *access-list-name* [{*access-list-number* **. . .** *access-list-name*}] | **prefix-list** *prefix-list-name* [*prefix-list-name* **. . .**]}
no match ip address {*access-list-number* [{*access-list-number* **. . .** | *access-list-name* **. . .**}] | *access-list-name* [{*access-list-number* **. . .** *access-list-name*}] | **prefix-list** *prefix-list-name* [*prefix-list-name* **. . .**]}

Syntax Description

access-list-number...	Number of a standard or extended access list. It can be an integer from 1 to 199. The ellipsis indicates that multiple values can be entered.
access-list-name...	Name of a standard or extended access list. It can be an integer from 1 to 199. The ellipsis indicates that multiple values can be entered.
prefix-list	Distributes routes based on a prefix list.
prefix-list-name...	Name of a specific prefix list. The ellipsis indicates that multiple values can be entered.

Command Default

No access list numbers or prefix lists are specified.

Command Modes

Route-map configuration (config-route-map)

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.
15.1(2)S	This command was integrated into Cisco IOS Release 15.1(2)S.

Usage Guidelines

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *access-list-number,access-list-name,orprefix-list-name*arguments .

Like matches in the same route map subblock are filtered with “or” semantics. If any one match clause is matched in the entire route map subblock, this match is treated as a successful match. Dissimilar match clauses are filtered with “and” semantics. So dissimilar matches are filtered logically. If the first set of conditions is not met, the second match clause is filtered. This process continues until a match occurs or there are no more match clauses.

Use route maps to redistribute routes or to subject packets to policy routing. Both purposes are described in this section.

Redistribution

Use the **route-map** global configuration command, and the **match** and **set** route-map configuration commands, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *matchcriteria*--the conditions under which redistribution is allowed for the current **route-map**command. The**set** commands specify the *setactions*--the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **noroute-map** command deletes the route map.

The **match** route-map configuration command has multiple formats. The **match** commands can be given in any order, and all **match** commands must “pass” to cause the route to be redistributed according to the *setactions*given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

When you are passing routes through a route map, a route map can have several sections that contain specific **match** clauses. Any route that does not match at least one **match** clause relating to a **route-map** command will be ignored; that is, the route will not be advertised for outbound route maps and will not be accepted for inbound route maps. If you want to modify only some data, you must configure a second route map section with an explicit match specified.

Policy Routing

Another purpose of route maps is to enable policy routing. The match ip address command allows you to policy route packets based on criteria that can be matched with an extended access list; for example, a protocol, protocol service, and source or destination IP address. To define the conditions for policy routing packets, use the **ippolicyroute-map** interface configuration command, in addition to the **route-map** global configuration command, and the **match** and **set** route-map configuration commands. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *matchcriteria*--the conditions under which policy routing occurs. The **set** commands specify the *setactions*--the particular routing actions to perform if the criteria enforced by the **match**commands are met. You might want to policy route packets based on their source, for example, using an access list.

Examples

In the following example, routes that have addresses specified by access list numbers 5 or 80 will be matched:

```
Router(config)# route-map name
Router(config-route-map)#  match ip address 5 80
```

Route maps that use prefix lists can be used for route filtering, default origination, and redistribution in other routing protocols. In the following example, a default route 0.0.0.0/0 is conditionally originated when there exists a prefix 10.1.1.0/24 in the routing table:

```
Router(config)# ip prefix-list cond permit 10.1.1.0/24
!
Router(config)# route-map default-condition permit 10
Router(config-route-map)# match ip address prefix-list cond
!
Router(config)# router rip
Router(config-router)# default-information originate route-map default-condition
```

In the following policy routing example, packets that have addresses specified by access list numbers 6 or 25 will be routed to Ethernet interface 0:

```
Router(config)# interface serial 0
Router(config-if)# ip policy route-map chicago
!
Router(config)# route-map chicago
Router(config-route-map)# match ip address 6 25
Router(config-route-map)# set interface ethernet 0
```

Related Commands

Command	Description
ip local policy route-map	Identifies a route map to use for policy routing on an interface.
ip policy route-map	Identifies a route map to use for policy routing on an interface.
match as-path	Matches a BGP autonomous system path access list.
match community	Matches a BGP community.
match interface (IP)	Distributes any routes that have their next hop out one of the interfaces specified.
match ip next-hop	Redistributes any routes that have a next hop router address passed by one of the access lists specified.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match length	Bases policy routing on the Level 3 length of a packet.
match metric (IP)	Redistributes routes with the metric specified.
match route-type (IP)	Redistributes routes of the specified type.
match tag	Redistributes routes in the routing table that match the specified tags.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set as-path	Modifies an autonomous system path for BGP routes.
set automatic-tag	Automatically computes the tag value.
set community	Sets the BGP communities attribute.
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Indicates where to output packets that pass a match clause of a route map for policy routing.
set ip default next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing and for which the Cisco IOS software has no explicit route to a destination.
set ip next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing.

Command	Description
set level (IP)	Indicates where to import routes.
set local-preference	Specifies a preference value for the autonomous system path.
set metric (BGP, OSPF, RIP)	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set next-hop	Specifies the address of the next hop.
set tag (IP)	Sets a tag value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.

match ip next-hop

To redistribute any routes that have a next hop router address passed by one of the access lists specified, use the **matchipnext-hop** command in route-map configuration mode. To remove the next hop entry, use the **no** form of this command.

match ip next-hop {*access-list-numberaccess-list-name*} [{. . . *access-list-number* | . . . *access-list-name*}]
no match ip next-hop {*access-list-numberaccess-list-name*} [{. . . *access-list-number* | . . . *access-list-name*}]

Syntax Description

access-list-number access-list-name	Number or name of a standard or extended access list. It can be an integer from 1 to 199.

Command Default

Routes are distributed freely, without being required to match a next hop address.

Command Modes

Route-map configuration (config-route-map)

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.
15.1(2)S	This command was integrated into Cisco IOS Release 15.1(2)S.

Usage Guidelines

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *access-list-numberoraccess-list-name* argument .

Use the route-map global configuration command, and the **match** and **set** route-map configuration commands, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *matchcriteria*--the conditions under which redistribution is allowed for the current route-mapcommand. The **set** commands specify the *setactions*--the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **noroute-map** command deletes the route map.

The **match** route-map configuration command has multiple formats. The **match** commands can be given in any order, and all **match** commands must "pass" to cause the route to be redistributed according to the *setactions*given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

When you are passing routes through a route map, a route map can have several parts. Any route that does not match at least one **match** clause relating to a **route-map** command will be ignored; that is, the route will not be advertised for outbound route maps and will not be accepted for inbound route maps. If you want to modify only some data, you must configure a second route map section with an explicit match specified.

Examples

The following example distributes routes that have a next hop router address passed by access list 5 or 80 will be distributed:

```
Router(config)# route-map name
Router(config-route-map)# match ip next-hop 5 80
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community	Matches a BGP community.
match interface (IP)	Distributes any routes that have their next hop out one of the interfaces specified.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match metric (IP)	Redistributes routes with the metric specified.
match route-type (IP)	Redistributes routes of the specified type.
match tag	Redistributes routes in the routing table that match the specified tags.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set as-path	Modifies an autonomous system path for BGP routes.
set automatic-tag	Automatically computes the tag value.
set community	Sets the BGP communities attribute.
set level (IP)	Indicates where to import routes.
set local-preference	Specifies a preference value for the autonomous system path.
set metric (BGP, OSPF, RIP)	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set next-hop	Specifies the address of the next hop.
set tag (IP)	Sets a tag value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.

match ip redistribution-source

To match the external Enhanced Interior Gateway Routing Protocol (EIGRP) routes that have been advertised by routers and access servers at the address specified by the access lists, use the **matchipredistribution-source** command in route-map configuration mode. To remove the redistribution-source entry, use the **no** form of this command.

match ip redistribution-source [*access-list-number* [**. . .** *access-list-number*]] [*expanded-access-list* [**. . .** *expanded-access-list*]] [*access-list-name* [**. . .** *access-list-name*]] [**prefix-list** *name* [**. . . prefix-list** *name*]]
no match ip redistribution-source [*access-list-number* [**. . .** *access-list-number*]] [*expanded-access-list* [**. . .** *expanded-access-list*]] [*access-list-name* [**. . .** *access-list-name*]] [**prefix-list** *name* [**. . . prefix-list** *name*]]

Syntax Description

access-list-number	(Optional) Number of a standard access list. The range is from 1 to 199.
expanded-access-list	(Optional) Number of an expanded access list. The range is from from 1300 to 1999.
access-list-name	(Optional) Name of a standard access list.
prefix-list *name*	(Optional) Specifies the match entries of a specified prefix list.

Command Default

No filtering of the routes is applied on the redistribution source.

Command Modes

Route-map configuration (config-route-map)

Command History

Release	**Modification**
15.1(3)T	This command was introduced in Cisco IOS Release 15.1(3)T.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S and implemented on Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *access-list-number*argument, the*expanded-access-list*argument, the*access-list-name*argument,and the **prefix-list***name*keyword and argument pair.

Use the **route-map** global configuration command, and the **match** and**set** route-map configuration commands, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the match criteria--the conditions under which redistribution is allowed for the current **route-map**command. The **set** commands specify the set actions--the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **noroute-map** command deletes the route map.

The **match** route-map configuration command has multiple formats. The **match** commands can be given in any order, and all **match** commands must “pass” to cause the route to be redistributed according to the set actionsgiven with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

Any route that does not match at least one **match** clause relating to a **route-map** command will be ignored; that is, the route will not be advertised for outbound route maps and will not be accepted for inbound route maps. If you want to modify only some data, you must configure the second route map section with an explicit match specified.

Examples

The following example shows how to filter the EIGRP routes that are advertised by routers and access servers at the address specified by access list 5 and expanded access list 1335:

```
Router(config)# route-map R1
Router(config-route-map)# match ip redistribution-source 5 1335
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community	Matches a BGP community.
match interface (IP)	Distributes any routes that have their next hop from one of the interfaces specified.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match ip route-source	Matches routes that have been advertised by routers and access servers at the address specified by the access lists.
match ip next-hop	Redistributes any routes that have a next hop router address passed by one of the access lists specified.
match metric (IP)	Redistributes routes with the metric specified.
match route-type (IP)	Redistributes routes of the specified type.
match tag	Redistributes routes in the routing table that match the specified tags.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set as-path	Modifies an autonomous system path for BGP routes.
set automatic-tag	Automatically computes the tag value.
set community	Sets the BGP communities attribute.
set level (IP)	Indicates where to import routes.
set local-preference	Specifies a preference value for the autonomous system path.
set metric (BGP, OSPF, RIP)	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set next-hop	Specifies the address of the next hop.

Command	Description
set tag (IP)	Sets a tag value for the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.

match ip route-source

To match routes that have been advertised by routers and access servers at the address specified by the access lists, use the **matchiproute-source** command in route-map configuration mode. To remove the route-source entry, use the **no** form of this command.

match ip route-source [*access-list-number* [. . . *access-list-number*]] [*expanded-access-list* [. . . *expanded-access-list*]] [*access-list-name* [. . . *access-list-name*]] [**prefix-list** *name* [. . . **prefix-list** *name*]] [**redistribution-source**]
no match ip route-source [*access-list-number* [. . . *access-list-number*]] [*expanded-access-list* [. . . *expanded-access-list*]] [*access-list-name* [. . . *access-list-name*]] [**prefix-list** *name* [. . . **prefix-list** *name*]] [**redistribution-source**]

Syntax Description

access-list-number	(Optional) Number of a standard access list. The range is from 1 to 199.
expanded-access-list	(Optional) Number of an expanded access list. The range is from 1300 to 1999.
access-list-name	(Optional) Name of a standard access list.
prefix-list *name*	(Optional) Configures the match entries of a specified prefix list.
redistribution-source	(Optional) Specifies the route redistribution source for Enhanced Interior Gateway Routing Protocol (EIGRP).

Command Default

No filtering of the routes is applied on the route source.

Command Modes

Route-map configuration (config-route-map)

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 and implemented on Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *access-list-number*argument,the*expanded-access-list*argument, the*access-list-name*argument,and the **prefix-list***name*keyword and argument pair.

Use the **route-map** global configuration command, and the **match** and**set** route-map configuration commands, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the match criteria--the conditions under which redistribution is allowed for the current **route-map**command. The **set** commands specify the set actions--the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **noroute-map** command deletes the route map.

The **match** route-map configuration command has multiple formats. The **match** commands can be given in any order, and all **match** commands must “pass” to cause the route to be redistributed according to the set actionsgiven with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

A route map can have several parts. Any route that does not match at least one **match** clause relating to a **route-map** command will be ignored; that is, the route will not be advertised for outbound route maps and will not be accepted for inbound route maps. If you want to modify only some data, you must configure the second route map section with an explicit match specified.

Examples

The following example shows how to match routes that are advertised by routers and access servers at the address specified by access list 5 and expanded access list 1335:

```
Router(config)# route-map R1
Router(config-route-map)# match ip route-source 5 1335
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community	Matches a BGP community.
match interface (IP)	Distributes any routes that have their next hop from one of the interfaces specified.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match ip redistribution-source	Filters the external EIGRP routes that have been advertised by routers and access servers at the address specified by the access lists.
match ip next-hop	Redistributes any routes that have a next hop router address passed by one of the access lists specified.
match metric (IP)	Redistributes routes with the metric specified.
match route-type (IP)	Redistributes routes of the specified type.
match tag	Redistributes routes in the routing table that match the specified tags.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set as-path	Modifies an autonomous system path for BGP routes.
set automatic-tag	Automatically computes the tag value.
set community	Sets the BGP communities attribute.
set level (IP)	Indicates where to import routes.

Command	Description
set local-preference	Specifies a preference value for the autonomous system path.
set metric (BGP, OSPF, RIP)	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set next-hop	Specifies the address of the next hop.
set tag (IP)	Sets a tag value for the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.

match ipv6 address

To distribute IPv6 routes that have a prefix permitted by a prefix list or to specify an IPv6 access list to be used to match packets for policy-based routing (PBR) for IPv6, use the **match ipv6 address** command in route-map configuration mode. To remove the **match ipv6 address** entry, use the **no** form of this command.

match ipv6 address {**prefix-list** *prefix-list-nameaccess-list-name*}
no match ipv6 address

Syntax Description

prefix-list *prefix-list-name*	Specifies the name of an IPv6 prefix list.
access-list-name	Name of the IPv6 access list. Names cannot contain a space or quotation mark or begin with a numeric.

Command Default

No routes are distributed based on the destination network number or an access list.

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.3(7)T	This command was modified. The *access-list-name* argument was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SXI4	This command was modified. The **prefix-list** *prefix-list-name* keyword-argument pair argument is not supported in Cisco IOS Release 12.2(33)SXI4.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

Use the **route-map** command and the **match** and **set** commands to define the conditions for redistributing routes from one routing protocol to another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the match criteria--the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions, which are the particular redistribution actions to be performed if the criteria enforced by the **match** commands are met.

The **match ipv6 address** command can be used to specify either an access list or a prefix list. When using PBR, you must use the *access-list-name* argument; the **prefix-list** *prefix-list-name* keyword-argument pair argument will not work.

Examples

In the following example, IPv6 routes that have addresses specified by the prefix list named marketing are matched:

```
Device(config)# route-map name
Device(config-route-map)# match ipv6 address prefix-list marketing
```

In the following example, IPv6 routes that have addresses specified by an access list named marketing are matched:

```
Device(config)# route-map
Device(config-route-map)# match ipv6 address marketing
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community	Matches a BGP community.
match ipv6 address	Specifies an IPv6 access list to be used to match packets for PBR for IPv6.
match ipv6 next-hop	Distributes IPv6 routes that have a next-hop prefix permitted by a prefix list.
match ipv6 route-source	Distributes IPv6 routes that have been advertised by routers at an address specified by a prefix list.
match length	Bases policy routing on the Level 3 length of a packet.
match metric	Redistributes routes with the specified metric.
match route-type	Redistributes routes of the specified type.
route-map	Defines conditions for redistributing routes from one routing protocol into another.
set as-path	Modifies an autonomous system path for BGP routes.
set community	Sets the BGP community attribute.
set default interface	Specifies the default interface to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Specifies the default interface to output packets that pass a match clause of a route map for policy routing.
set ipv6 default next-hop	Specifies an IPv6 default next hop to which matching packets will be forwarded.
set ipv6 next-hop (PBR)	Indicates where to output IPv6 packets that pass a match clause of a route map for policy routing.
set ipv6 precedence	Sets the precedence value in the IPv6 packet header.

Command	Description
set level	Indicates where to import routes.
set local preference	Specifies a preference value for the autonomous system path.
set metric	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set tag	Sets a tag value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.

match length

To base policy routing on the Level 3 length of a packet, use the **match length** command in route-map configuration mode. To remove the entry, use the **no** form of this command.

match length *minimum-length maximum-length*
no match length *minimum-length maximum-length*

Syntax Description

minimum-length	Minimum Level 3 length of the packet allowed for a match. The range is from 0 to 0x7FFFFFFF.
maximum-length	Maximum Level 3 length of the packet allowed for a match. The range is from 0 to 0x7FFFFFFF.

Command Default

No policy routing occurs on the length of a packet.

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
10.0	This command was introduced.
12.3(7)T	This command was modified. This command was updated for use in configuring IPv6 policy-based routing (PBR).
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

In IPv4, use the **ip policy route-map** interface configuration command, the **route-map** global configuration command, and the **match** and **set** route-map configuration commands to define the conditions for policy routing packets. The **ip policy route-map** command identifies a route map by name. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the **match criteria**—the conditions under which policy routing occurs. The **set** commands specify the **set actions**—the particular routing actions to perform if the criteria enforced by the **match** commands are met.

In PBR for IPv6, use the **ipv6 policy route-map** or **ipv6 local policy route-map** command to define conditions for policy routing packets.

In IPv4, the **match** route-map configuration command has multiple formats. The **match** commands can be issued in any order, and all **match** commands must “pass” to cause the packet to be routed according to the **set actions** given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

In IPv4, you might want to base your policy routing on the length of packets so that your interactive traffic and bulk traffic are directed to different routers.

Examples

In the following example, packets 3 to 200 bytes long, inclusive, will be routed to FDDI interface 0:

```
interface serial 0
 ip policy route-map interactive
!
route-map interactive
 match length 3 200
 set interface fddi 0
```

In the following example for IPv6, packets 3 to 200 bytes long, inclusive, will be routed to FDDI interface 0:

```
interface Ethernet0/0
  ipv6 policy-route-map interactive
!
route-map interactive
 match length 3 200
 set interface fddi 0
```

Related Commands

Command	Description
ip local policy route-map	Identifies a route map to be used for policy routing on an interface.
ipv6 local policy route-map	Configures IPv6 PBR for IPv6 originated packets.
ipv6 policy route-map	Configures IPv6 PBR on an interface.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match ipv6 address	Specifies an IPv6 access list to be used to match packets for IPv6 PBR.
match length	Bases policy routing on the Level 3 length of a packet.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol to another, or enables policy routing.
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Indicates where to output packets that pass a match clause of route map for policy routing.
set ip default next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing and for which the Cisco software has no explicit route to a destination.
set ipv6 default next-hop	Specifies an IPv6 default next hop to which matching packets will be forwarded.
set ip next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing.

Command	Description
set ipv6 next-hop (PBR)	Indicates where to output IPv6 packets that pass a match clause of a route map for policy routing.
set ipv6 precedence	Sets the precedence value in the IPv6 packet header.

match metric (IP)

To redistribute r outes with the specified metric, use the **matchmetric** command in route-map configuration mode. To remove the entry for the redistributed route from the routing table, use the **no** form of this command.

match metric {*metric-value* | **external** *metric-value*} [+-*deviation-number*]
no match metric {*metric-value* | **external** *metric-value*} [+-*deviation-number*]

Syntax Description

metric-value	Internal route metric, which can be an Enhanced Interior Gateway Routing Protocol (EIGRP) five-part metric. The range is from 1 to 4294967295.
external	External protocol associated with a route and interpreted by a source protocol.
+- *deviation-number*	(Optional) A standard deviation number that will offset the number configured for the metric-value argument. The deviation-number argument can be any number. There is no default. **Note** When you specify a deviation of the metric with the **+** and **-** keywords, the router will match any metric that falls inclusively in that range.

Command Default

No filtering is performed on a metric value.

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
11.2	This command was introduced.
12.3(8)T	The **external** and **+-**keywords and *deviation-number* argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Use the **route-map** global configuration command and the **match** and **set** route-map configuration commands to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *matchcriteria*--the conditions under which redistribution is allowed for the current **route-map**command. The **set** commands specify the *setactions*--the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **noroute-map** command deletes the route map.

The **match** route-map configuration command has multiple formats. The **match** commands can be given in any order, and all **match** commands must "pass" to cause the route to be redistributed according to the set actionsgiven with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

A route map can have several parts. Any route that does not match at least one **match** clause relating to a **route-map**command will be ignored; that is, the route will not be advertised for outbound route maps and will not be accepted for inbound route maps. If you want to modify only some data, you must configure a second route map section with an explicit match specified.

Note An external protocol route metric is not the same as the EIGRP assigned route metric which is a figure computed using EIGRP vectorized metric components (delay, bandwidth, reliability, load, and MTU).

Examples

In the following example, routes with the metric 5 will be redistributed:

```
Router(config)# route-map name
Router(config-route-map)# match metric 5
```

In the following example, any metric that falls inclusively in the range from 400 to 600 is matched:

```
Router(config)# route-map name
Router(config-route-map)# match metric 500 +- 100
```

The following example shows how to configure a route map to match an EIGRP external protocol metric route with an allowable deviation of 100, a source protocol of BGP, and an autonomous system 45000. When the two match clauses are true, the tag value of the destination routing protocol is set to 5. The route map is used to distribute incoming packets for an EIGRP process.

```
Router(config)# route-map metric_range
Router(config-route-map)# match metric external 500 +- 100
Router(config-route-map)# match source-protocol bgp 45000
Router(config-route-map)# set tag 5
!
Router(config)# router eigrp 45000
Router(config-router)# network 172.16.0.0
Router(config-router)# distribute-list route-map metric_range in
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community	Matches a BGP community.
match interface (IP)	Distributes any routes that have their next hop out one of the interfaces specified.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match ip next-hop	Redistributes any routes that have a next hop router address passed by one of the access lists specified.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match route-type (IP)	Redistributes routes of the specified type.
match tag	Redistributes routes in the routing table that match the specified tags.

Command	Description
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set as-path	Modifies an autonomous system path for BGP routes.
set automatic-tag	Automatically computes the tag value.
set community	Sets the BGP communities attribute.
set level (IP)	Indicates where to import routes.
set local-preference	Specifies a preference value for the autonomous system path.
set metric (BGP, OSPF, RIP)	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set next-hop	Specifies the address of the next hop.
set tag (IP)	Sets a tag value of the destination routing protocol.

match route-type (IP)

To redistribute routes of the specified type, use the **matchroute-type** command in route-map configuration mode. To remove the route type entry, use the **no** form of this command.

match route-type {**local** | **internal** | **external** [{**type-1** | **type-2**}] | **level-1** | **level-2**}
no match route-type {**local** | **internal** | **external** [{**type-1** | **type-2**}] | **level-1** | **level-2**}

Syntax Description

local	Locally generated Border Gateway Protocol (BGP) routes.
internal	Open Shortest Path First (OSPF) intra-area and interarea routes or Enhanced Interior Gateway Routing Protocol (EIGRP) internal routes.
external [**type-1**|**type-2**	OSPF external routes, or EIGRP external routes. For OSPF, the **externaltype-1** keyword matches only Type 1 external routes and the **externaltype-2** keyword matches only Type 2 external routes.
level-1	Intermediate System-to-Intermediate System (IS-IS) Level 1 routes.
level-2	IS-IS Level 2 routes.

Command Default

This command is disabled by default.

Command Modes

Route-map configuration

Command History

Release	Modification
10.0	This command was introduced.
11.2	The **local** and **external** [**type-1** | **type-2**] keywords were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **route-map** global configuration command, and the **match** and **set** route-map configuration commands, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *matchcriteria*--the conditions under which redistribution is allowed for the current **route-map**command. The **set** commands specify the *setactions*--the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **noroute-map** command deletes the route map.

The **match** route-map configuration command has multiple formats. The **match** commands can be given in any order, and all **match** commands must “pass” to cause the route to be redistributed according to the *setactions*given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

A route map can have several parts. Any route that does not match at least one **match** clause relating to a **route-map** command will be ignored; that is, the route will not be advertised for outbound route maps and will not be accepted for inbound route maps. If you want to modify only some data, you must configure second route map section with an explicit match specified.

Examples

The following example redistributes internal routes:

```
route-map name
 match route-type internal
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community	Matches a BGP community.
match interface (IP)	Distributes any routes that have their next hop out one of the interfaces specified.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match ip next-hop	Redistributes any routes that have a next hop router address passed by one of the access lists specified.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match metric (IP)	Redistributes routes with the metric specified.
match tag	Redistributes routes in the routing table that match the specified tags.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set as-path	Modifies an autonomous system path for BGP routes.
set automatic-tag	Automatically computes the tag value.
set community	Sets the BGP communities attribute.
set level (IP)	Indicates where to import routes.
set local-preference	Specifies a preference value for the autonomous system path.
set metric (BGP, OSPF, RIP)	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set next-hop	Specifies the address of the next hop.
set tag (IP)	Sets a tag value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.

match tag

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

match tag {*tag-valuetag-value-dotted-decimal*} [. . . *tag-value* | . . . *tag-value-dotted-decimal*]
no match tag {*tag-valuetag-value-dotted-decimal*} [. . . *tag-value* | . . . *tag-value-dotted-decimal*]

Syntax Description

tag-value	Route tag value in plain decimals. The valid range is from 0 to 4294967295.
tag-value-dotted-decimal	Route tag value in dotted decimals. The valid range is from 0.0.0.0 to 255.255.255.255.

Command Default

No match tag values are defined.

Command Modes

Route-map configuration (config-route-map)

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 implemented on Cisco ASR 1000 Series Aggregation Services Routers.
15.1(2)S	This command was integrated into Cisco IOS Release 15.1(2)S.
15.2(2)S	This command was modified. The *tag-value-dotted-decimal* argument was added to support tag values in dotted-decimal format.
Cisco IOS XE Release 3.6S	This command was modified. The *tag-value-dotted-decimal* argument was added to support tag values in dotted-decimal format.

Usage Guidelines

Ellipses (...) in the command syntax indicate that your command input can include multiple values for the *tag-value* and the *tag-value-dotted-decimal* arguments.

Examples

The following example shows how to match a route with a tag value of 5:

```
Device(config)# route-map name
Device(config-route-map)# match tag 5
```

The following example shows how to match a route with a tag value of 10.10.10.10:

```
Device(config)# route-map name
Device(config-route-map)# match tag 10.10.10.10
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path specified by an access list.
match community	Matches a BGP community.
match ip address	Distributes any route that has a destination address that performs policy routing on packets and is permitted by a standard or extended access list.
route-map (IP)	Defines conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set automatic-tag	Automatically computes the tag value.
set level (IP)	Indicates where to import routes.
set local-preference	Specifies a preference value for autonomous system paths that pass a route map.
set metric (BGP-OSPF-RIP)	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set next-hop	Specifies the address of the next hop.
set tag (IP)	Sets a tag value for a route.

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.

match track

To enable tracking of a stub object during Policy-Based Routing (PBR), use the **match track** command in route-map configuration mode. To disable tracking of the stub object, use the **no** form of the command.

match track *track-object-number*
no **match track** *track-object-number*

Syntax Description

track-object-number	Number of the stub object that you want to track. The range is from 1 to 1000.

Command Default

Stub object is not tracked.

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
15.4(3)M	This command was introduced.
Cisco IOS XE Release 3.13S	This command was integrated into Cisco IOS XE Release 3.13S.

Usage Guidelines

The **match track** command also verifies the existence of the stub object that you want to track. The device checks for the existence of the match track object and issues an error message if there is none. Then registration with the tracking component is done to track this object. The device issues an error in case the registration fails.

Example

The following example shows how to enable tracking of a stub object during Policy-Based Routing (PBR):

```
Device> enable
Device# configure terminal
Device(config)# route-map abc
Device(config-route-map)# match track 2
Device(config-route-map)# end
```

Related Commands

Command	Description
route-map	Defines conditions for redistributing routes from one routing protocol into another routing protocol, or to enable policy routing.
show route-map	Displays the configured route maps.

maximum-paths

To control the maximum number of parallel routes that an IP routing protocol can support, use the **maximum-paths** command in router address family topology or router configuration mode. To restore the default number of parallel routes, use the **no** form of this command.

maximum-paths *number-of-paths*
no maximum-paths *number-of-paths*

Syntax Description

number-of-paths	Maximum number of parallel routes that an IP routing protocol installs in a routing table. Valid values vary by Cisco IOS release and platform. For more information on valid values, use the question mark (**?**) online help function.

Command Default

The default number of parallel routes vary by Cisco IOS release and platform.

Command Modes

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

Router configuration (config-router)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(14)SX	This command was implemented on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was modified. This command was made available in router address family topology configuration mode.
12.2(33)SXH	This command was modified. The maximum number of paths was changed from 8 to 16 for Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 3.5S	In Cisco IOS XE Release 3.5S, support was added for the Cisco ASR 903 Router.

Usage Guidelines

Release 12.2(33)SRB

If you plan to configure the Multi-Topology Routing (MTR) feature, you need to enter the **maximum-paths** command in router address family topology configuration mode for this Open Shortest Path First (OSPF) router configuration command to become aware of the topology.

Examples

The following example shows how to allow a maximum of 16 paths to a destination in an OSPF routing process:

```
Router(config)# router ospf 3
Router(config-router)# maximum-paths 16
```

monitor peer bfd

To enable pseudowire fast-failure detection capability in a bidirectional forwarding detection (BFD) configuration, use the **monitor peer bfd** command in the appropriate configuration mode. To disable pseudowire fast-failure detection, use the **no** form of this command.

monitor peer bfd [**local interface** *interface-type*]
no monitor peer bfd [**local interface**]

Syntax Description

local interface *interface-type*	(Optional) Specifies the local interface for the source address to use when locating a BFD configuration.

Command Default

Pseudowire fast-failure detection is disabled.

Command Modes

Interface configuration (config-if)

Pseudowire class configuration (config-pw-class)

Template configuration (config-template)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.6S	This command was integrated into a release prior to Cisco IOS XE Release 3.6S.
Cisco IOS XE Release 3.7S	This command was modified as part of the MPLS-based Layer 2 VPN (L2VPN) command modifications for cross-OS support. This command was made available in interface configuration and template configuration modes.

Examples

The following example shows how to enable pseudowire fast-failure detection capability:

```
Device(config)# interface Loopback0
Device(config-if)# ip address 10.1.1.1 255.255.255.255
Device(config-if)# exit
Device(config)# pseudowire-class mpls
Device(config-pw-class)# encapsulation mpls
Device(config-pw-class)# monitor peer bfd local interface Loopback0
```

The following example shows how to enable pseudowire fast-failure detection capability in interface configuration mode:

```
Device(config)# interface pseudowire 100
Device(config-if)# encapsulation mpls
Device(config-if)# monitor peer bfd local interface gigabitethernet0/0/0
```

The following example shows how to enable pseudowire fast-failure detection capability in template configuration mode:

```
Device(config)# template type pseudowire 1
Device(config-template)# encapsulation mpls
Device(config-template)# monitor peer bfd local interface gigabitethernet0/0/0
```

Related Commands

Command	Description
bfd map	Configures a BFD map that associates timers and authentication with multihop templates.
bfd-template	Creates a BFD template and enters BFD configuration mode.
encapsulation (Any Transport over MPLS)	Configures the AAL encapsulation for AToM.
encapsulation (pseudowire)	Specifies an encapsulation type for tunneling Layer 2 traffic over a pseudowire.
pseudowire-class	Specifies the name of a Layer 2 pseudowire class.

named-ordering-route-map enable

To enable ordering of route maps based on a sequence string, use the **named-ordering-route-map enable** command in the global configuration mode. To disable ordering of route maps based on a sequence string, use the **no** form of this command.

named-ordering-route-map enable
no named-ordering-route-map

Syntax Description

This command has no arguments or keywords.

Command Default

By default ordering of route maps based on sequence string is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced in this release.

Examples

The following example shows how to enable ordering of route maps based on a sequence string:

```
Device# config
Device(config)# named-ordering-route-map enable
```

nsf

To enable and configure Cisco NSF, use the **nsf** command in router configuration mode. To disable NSF, uses the **no** form of this command.

nsf [**enforce global**]
nsf [{{**cisco** | **ietf**} | **interface wait** *seconds* | **interval** *minutes* | **t3** [{**adjacency** | **manual** *seconds*}]}]
no nsf

Syntax Description

enforce global	(Optional) Cancels OSPF NSF restart when non-NSF-aware neighbors are detected.
cisco	Specifies the Cisco proprietary IS-IS NSF method of checkpointing if the active RP fails over.
ietf	Specifies the IETF IS-IS NSF method of protocol modification if the active RP fails over.
interface wait *seconds*	(Optional) Specifies how long to wait for an interface to come up after failover before it proceeds with the Cisco NSF process; valid values are from 1 to 60 seconds.
interval *minutes*	(Optional) Specifies how long to wait after a route processor stabilizes before restarting; valid values are from 0 to 1440 minutes.
t3 adjacency	(Optional) Specifies that the time that IETF NSF waits for the LSP database to synchronize is determined by the adjacency holdtime advertised to the neighbors of the specified RP before switchover.
t3 manual *seconds*	(Optional) Specifies the time to wait after the NSF database synchronizes before informing other nodes to remove the restarting node from consideration as a transit; valid values are from 5 to 3600 seconds.

Command Default

The default settings are as follows:

- NSF is disabled.
- **enforce global** --Enabled.
- interval *minutes*--5 minutes.
- interface **wait***seconds*--10 seconds.
- t3 manual *seconds*--30 seconds.

Command Modes

Router configuration

Command History

Release	Modification
12.2(18)SXD	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
15.2(1)E	This command was integrated into Cisco IOS Release 15.2(1)E.

Usage Guidelines

The **nsf** command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

The **nsfinterfacewait**command can be used if Cisco proprietary IS-IS NSF is configured or if the Internet Engineering Task Force (IETF) IS-IS NSF is enabled using the **nsft3** manual command. You can use this command if an interface is slow to come up.

Note

Cisco NSF is required only if the Cisco 7600 series router is expected to perform Cisco NSF during a restart. If the Cisco 7600 series router is expected to cooperate with a neighbor that is doing a Cisco NSF restart only, the switch must be NSF capable by default (running a version of code that supports Cisco NSF), but Cisco NSF does not have to be configured on the switch.

The **nsf** commands are a subset of the **router** command and affects all the interfaces that are covered by the designated process. Cisco NSF supports the BGP, OSPF, IS-IS, and EIGRP protocols. The configuration commands that enable NSF processing are as follows:

- **nsf** under the **routerospf** command
- **nsf ietf** under the **routerisis** command
- **bgp graceful-restart** under the **routerbgp** command

These commands must be issued as part of the router's running configuration. During the restart, these commands are restored to activate the NSF processing.

The [{cisco | ietf } | interface **wait***seconds* | interval *minutes* | t3 [adjacency | manual *seconds*] keywords and arguments apply to IS-IS only.

The {**enforceglobal**} keywords apply to OSPF only.

BGP NSF Guidelines

BGP support in NSF requires that neighbor networking devices be NSF-aware devices; that is, they must have the graceful restart capability and advertise that capability in the OPEN message during session establishment. If an NSF-capable router discovers that a particular BGP neighbor does not have the graceful restart capability enabled, it will not establish an NSF-capable session with that neighbor. All other neighbors that have a graceful restart capability will continue to have NSF-capable sessions with this NSF-capable networking device. Enter the **bgpgraceful-restart** router configuration command to enable the graceful restart capability.

EIRGP NSF Guidelines

A router may be an NSF-aware router but may not be participating in helping out the NSF restarting neighbor because it is coming up from a cold start.

IS-IS NSF Guidelines

If you configure IETF on the networking device, but neighbor routers are not IETF-compatible, NSF will terminate after the switchover.

Use these two keywords when configuring IS-IS NSF:

- **ietf** --Internet Engineering Task Force IS-IS--After a supervisor engine switchover, the NSF-capable router sends the IS-IS NSF restart requests to the neighboring NSF-aware devices.
- **cisco** --Cisco IS-IS. Full adjacency and LSP information is saved (checkpointed) to the standby supervisor engine. After a switchover, the newly active supervisor engine maintains its adjacencies using the checkpointed data to quickly rebuild its routing tables.

OSPF NSF Guidelines

OSPF NSF requires that all neighbor networking devices be NSF-aware devices. If an NSF-capable router discovers that it has non-NSF aware neighbors on a particular network segment, it will disable the NSF capabilities for that segment. The other network segments that are composed entirely of NSF-capable or NSF-aware routers will continue to provide NSF capabilities.

OSPF NSF supports NSF/SSO for IPv4 traffic only. OSPFv3 is not supported with NSF/SSO. Only OSPFv2 is supported with NSF/SSO.

Examples

This example shows how to enable NSF for all OSPF-process interfaces:

```
Router(config)# router ospf 109
Router(config-router)# nsf
```

This example shows how to disable NSF for all OSPF-process interfaces:

```
Router(config)# router ospf 109
Router(config-router)# no nsf
```

Related Commands

Command	Description
router	Enables a routing process.

passive-interface

To disable sending routing updates on an interface, use the **passive-interface** command in router configuration mode. To re-enable the sending of routing updates, use the **no** form of this command.

passive-interface commandpassive-interface [**default**] **i** *nterface-type interface-number*
no passive-interface *interface-type interface-number*

Syntax Description

default	(Optional) Causes all interfaces to become passive.
interface-type	Interface type.
interface-number	Interface number.

Command Default

Routing updates are sent on the interface.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
10.0	This command was introduced.
12.0	This command was modified. The **default** keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.1(2)S	This command was integrated into Cisco IOS Release 15.1(2)S.

Usage Guidelines

If you disable the sending of routing updates on an interface, the particular subnet will continue to be advertised to other interfaces, and updates from other routers on that interface continue to be received and processed.

The **default** keyword sets all interfaces as passive by default. You can then configure individual interfaces where adjacencies are desired using the **nopassive-interface** command. The **default** keyword is useful in Internet service provider (ISP) and large enterprise networks where many of the distribution routers have more than 200 interfaces.

For the Open Shortest Path First (OSPF) protocol, OSPF routing information is neither sent nor received through the specified router interface. The specified interface address appears as a stub network in the OSPF domain.

For the Intermediate System-to-Intermediate System (IS-IS) protocol, this command instructs IS-IS to advertise the IP addresses for the specified interface without actually running IS-IS on that interface. The **no** form of this command for IS-IS disables advertising IP addresses for the specified address.

Note For IS-IS you must keep at least one active interface and configure the interface with the **iprouterisis** command.

The use of the **passive-interface** command in Enhanced Interior Gateway Routing Protocol (EIGRP) suppresses the exchange of hello packets on the interface and thus stops routing updates from being advertised, and it also suppresses incoming routing updates. For more information on passive interfaces, see http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080093f0a.shtml .

Examples

The following example sends EIGRP updates to all interfaces on network 10.108.0.0 except Ethernet interface 1:

```
router eigrp 109
 network 10.108.0.0
 passive-interface ethernet 1
```

The following configuration enables IS-IS on Ethernet interface 1 and serial interface 0 and advertises the IP addresses of Ethernet interface 0 in its link-state protocol data units (PDUs):

```
router isis Finance
 passive-interface Ethernet 0
interface Ethernet 1
 ip router isis Finance
interface serial 0
 ip router isis Finance
```

The following example sets all interfaces as passive and then activates Ethernet interface 0:

```
router ospf 100
 passive-interface default
 no passive-interface ethernet0
 network 10.108.0.1 0.0.0.255 area 0
```

platform bfd allow-svi

To allow Bidirectional Forwarding Detection (BFD) configuration on a VLAN Switched Virtual Interface (SVI), use the platform bfd allow-svi command in global configuration mode. To disable BFD configuration on a VLAN SVI, use the no form of this command.

platformbfd allow-svi

Syntax Description

This command has no arguments or keywords.

Command Default

BFD configuration on VLAN SVIs is not allowed.

Command Modes

Global configuration (config)#

Command History

Release	Modification
15.0(1)S	This command was introduced.
15.1(1)SG	This command was integrated into Cisco IOS 15.1(1)SG.

Usage Guidelines

BFD over SVI configuration is allowed only when the platform bfd allow-svi hidden command has been configured. When this command is first issued, the system displays a warning message stating that BFD over SVI is not generically supported.

The no form of the command can be issued even if BFD over SVI configuration is present on the router. After the no form of the command is issued, no further BFD over SVI configuration is allowed.

Note You should unconfigure all BFD over SVI sessions before you issue the no platform allow-svi command.

Examples

The following example shows how to allow BFD configuration on a VLAN SVI:

```
Router# configure terminal
 Router(config)# platform bfd allow-svi
 Router(config)# interface vlan 100
 Router(config-if)# bfd interval 500 min_rx 500 multiplier 4
```

Related Commands

Command	Description
bfd	Sets the baseline BFD session parameters on an interface.
bfd all-interfaces	Enables BFD for all interfaces for a BFD peer.
bfd interface	Enables BFD on a per-interface basis for a BFD peer.
interface	Configures an interface type and enters interface configuration mode.

platform bfd enable-offload

To enable a BFD session offload on a system, use the **platformbfdenable-offload** command in the global configuration mode. To disable the BFD session offload use the **no** form of this command.

platform bfd enable-offload
no platform bfd enable-offload

Syntax Description

This command has no arguments or keywords

Command Default

Command is disabled.

Command Modes

Global configuration (config)#

Command History

Release	Modification
15.1(2)S	This command was introduced.
Cisco IOS XE Release 3.6S	This command was integrated.

Usage Guidelines

The BFD sessions running in IOS prior to configuring this command are not affected. All the BFD sessions initialized after you use this command are offloaded to the ES+ line card provided all the required parameters are met. For more information about BFD, see Configuring Layer 1 and Layer 2 Features .

Examples

This example shows how to enable BFD session offload to the ES+ line card:

```
Router(config)# platform bfd enable-offload
```

platform cloudsec padding-fixup

To configure the CloudSec padding-fixup dst-udp-port and debug parameters, use the **platformcloudsecpadding-fixup** command in the global configuration mode. To disable this command, use the **no** form of this command.

platform cloudsec padding-fixup { **dst-udp-port** *1st port number* [*2nd port number*] [*3rd port number*] | **debug** }
no platform cloudsec padding-fixup { **dst-udp-port** | **debug** }

Syntax Description

padding-fixup	Specifies the fixup for the small CloudSec packets with padding length.
dst-udp-port	Specifies the UDP destination port numbers for CloudSec packets.
1st port number	Specifies the 1st UDP destination port. Valid values are from 1024 to 49151.
2nd port number	(Optional) Specifies the 2nd UDP destination port. Valid values are from 1024 to 49151.
3rd port number	(Optional) Specifies the 3rd UDP destination port. Valid values are from 1024 to 49151.
debug	Specifies the CloudSec debug.

Command Default

Command is disabled.

Command Modes

Global configuration (config)#

Command History

Release	Modification
Cisco IOS XE Release 17.6.1	This command was introduced on the Cisco ASR 1000 Series Routers.

Usage Guidelines

Use the **platform cloudsec padding-fixup dst-udp-port** command to configure up to 3 UDP destination ports for CloudSec packets. Use the **platform cloudsec padding-fixup debug** command to enable the CloudSec debug.

To fix the ACI CloudSec encryption technology issue on the Cisco Nexus 9000 Series platforms, the ASR 1000 platforms provide a workaround solution that introduces new commands for CloudSec in platform specific configuration and the new commands are only applicable for the Nexus 9000 CloudSec Encryption feature. For more details, see CloudSec Encryption .

Examples

The following example shows how to configure the CloudSec padding-fixup dst-udp-port and debug:

```
Device# configure terminal
Device(config)# platform cloudsec padding-fixup dst-udp-port 9999 5120 8017
Device(config)# platform cloudsec padding-fixup debug
```

Related Commands

Command	Description
show platform software ip rp active cloudsec	Show command for displaying Cloudsec configurations in RP.
show platform software ip fp active cloudsec	Show command for displaying Cloudsec configurations in FP.

recv-id

Specifies the receive ID for a TCP-AO key chain.

recv-id *ID*

Syntax Description

ID	Specifies the receive identifier. An integer between 0 to 255.

Command Default

No key chain exists.

Command Modes

Key chain key configuration (config-keychain-key)

Command History

Release	Modification
16.12.1	This command was introduced.

Usage Guidelines

The **send-id** on the device must match the **recv-id** on the other device and vice versa.

You must configure a key chain with keys to enable authentication.

Although you can identify multiple key chains, we recommend using one key chain per interface per routing protocol. Upon specifying the **key chain** command, you enter key chain configuration mode.

The following example configures a simple key chain for a TCP-AO enabled connection.

```
Router(config)# key chain kc1 tcp
Router(config-keychain)# key 7890
Router(config-keychain-key)# send-id 215
Router(config-keychain-key)# recv-id 215
Router(config-keychain-key)# key-string klomn
Router(config-keychain-key)# cryptographic-algorithm hmac-sha-1
Router(config-keychain-key)# include-tcp-options
```

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

redistribute (IP)

To redistribute routes from one routing domain into another routing domain, use the **redistribute** command in the appropriate configuration mode. To disable all or some part of the redistribution (depending on the protocol), use the **no** form of this command. See the “Usage Guidelines” section for detailed, protocol-specific behaviors.

redistribute *protocol* [*process-id*] { **level-1** | **level-1-2** | **level-2** } [*autonomous-system-number*] [**metric** { *metric-value* | **transparent** }] [**metric-type** *type-value*] [**match** { **internal** | **external 1** | **external 2** }] [**tag** *tag-value*] [**route-map** *map-tag*] [**registered**] [**resolved**] [**summary**] [**subnets**] [**nssa-only**]
no redistribute *protocol* [*process-id*] {**level-1** | **level-1-2** | **level-2**} [*autonomous-system-number*] [**metric** {*metric-value* | **transparent**}] [**metric-type** *type-value*] [**match** {**internal** | **external 1** | **external 2**}] [**tag** *tag-value*] [**route-map** *map-tag*] [**registered**] [**resolved**] [**summary**] [**subnets**] [**nssa-only**]

Syntax Description

protocol	Source protocol from which routes are being redistributed. It can be one of the following keywords: **application**, **bgp**, **connected**, **eigrp**, **isis**, **mobile**, **ospf**, **rip**, **nhrp**, or **static** [**ip**]. The **static** [**ip**] keyword is used to redistribute IP static routes. The optional **ip** keyword is used when redistributing into the Intermediate System-to-Intermediate System (IS-IS) protocol. The **application** keyword is used to redistribute an application from one routing domain to another. In Cisco IOS XE Release 3.12S and Cisco IOS Release 15.4(3)M, you can redistribute more than one application to different routing protocols such as IS-IS, OSPF, Border Gateway Protocol (BGP), Enhanced Interior Gateway Routing Protocol (EIGRP) and Routing Information Protocol (RIP). The **connected** keyword refers to routes that are established automatically by virtue of having enabled IP on an interface. For routing protocols such as Open Shortest Path First (OSPF) and IS-IS, these routes will be redistributed as external to the autonomous system.

process-id	(Optional) For the **application** keyword, this is the name of an application. For the **bgp** or **eigrp** keyword, this is an autonomous system number, which is a 16-bit decimal number. For the **isis** keyword, this is an optional *tag* value that defines a meaningful name for a routing process. Creating a name for a routing process means that you use names when configuring routing. You can configure a router in two routing domains and redistribute routing information between these two domains. For the **ospf** keyword, this is an appropriate OSPF process ID from which routes are to be redistributed. This identifies the routing process. This value takes the form of a nonzero decimal number. For the **nhrp** keyword, this is an appropriate NHRP process ID from which routes are to be redistributed. This identifies the routing process. This value takes the form of a nonzero decimal number. For the **rip** keyword, no *process-id* value is needed. For the **application** keyword, this is the name of an application. By default, no process ID is defined.
level-1	Specifies that, for IS-IS, Level 1 routes are redistributed into other IP routing protocols independently.
level-1-2	Specifies that, for IS-IS, both Level 1 and Level 2 routes are redistributed into other IP routing protocols.
level-2	Specifies that, for IS-IS, Level 2 routes are redistributed into other IP routing protocols independently.
autonomous-system-number	(Optional) Autonomous system number for the redistributed route. The range is from 1 to 65535. • In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, 4-byte autonomous system numbers are supported in the range from 65536 to 4294967295 in asplain notation and in the range from 1.0 to 65535.65535 in asdot notation. • In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, 4-byte autonomous system numbers are supported in the range from 1.0 to 65535.65535 in asdot notation only. For more details about autonomous system number formats, see the **router bgp** command.

metric *metric-value*	(Optional) When redistributing from one OSPF process to another OSPF process on the same router, the metric will be carried through from one process to the other if no metric value is specified. When redistributing other processes to an OSPF process, the default metric is 20 when no metric value is specified. The default value is 0. (Optional) When redistributing from one NHRP process to another routing process on the same router, the metric will be carried through from one process to the other if no metric value is specified. The default value is 0.
metric transparent	(Optional) Causes RIP to use the routing table metric for redistributed routes as the RIP metric.
metric-type *type value*	(Optional) For OSPF, specifies the external link type associated with the default route advertised into the OSPF routing domain. It can be one of two values: • **1**—Type 1 external route • **2**—Type 2 external route If a **metric-type** is not specified, the Cisco IOS software adopts a Type 2 external route. For IS-IS, it can be one of two values: • **internal**—IS-IS metric that is < 63. • **external**—IS-IS metric that is > 64 < 128. The default is **internal**.
match {**internal** | **external1** | **external2**}	(Optional) Specifies the criteria by which OSPF routes are redistributed into other routing domains. It can be one of the following: • **internal**—Routes that are internal to a specific autonomous system. • **external 1**—Routes that are external to the autonomous system, but are imported into OSPF as Type 1 external routes. • **external 2**—Routes that are external to the autonomous system, but are imported into OSPF as Type 2 external routes. The default is **internal**.

tag *tag-value*	(Optional) Specifies the 32-bit decimal value attached to each external route. This is not used by OSPF itself. It may be used to communicate information between Autonomous System Boundary Routers (ASBRs). If none is specified, the remote autonomous system number is used for routes from BGP and Exterior Gateway Protocol (EGP); for other protocols, zero (0) is used.
route-map	(Optional) Specifies the route map that should be interrogated to filter the importation of routes from this source routing protocol to the current routing protocol. If not specified, all routes are redistributed. If this keyword is specified, but no route map tags are listed, no routes will be imported.
map-tag	(Optional) Identifier of a configured route map.
registered	(Optional) Limit redistribution to registered NHRP routes.
resolved	(Optional) Limit redistribution to resolved NHRP routes.
summary	(Optional) Limit redistribution to NHRP summary routes.
subnets	(Optional) For redistributing routes into OSPF, the scope of redistribution for the specified protocol. By default, no subnets are defined.
nssa-only	(Optional) Sets the nssa-only attribute for all routes redistributed into OSPF.

Command Default

Route redistribution is disabled.

Command Modes

Router configuration (config-router)

Address family configuration (config-af)

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

Command History

Release	Modification
10.0	This command was introduced.
12.0(5)T	This command was modified. Address family configuration mode was added.
12.0(22)S	This command was modified. Address family support under EIGRP was added.
12.2(15)T	This command was modified. Address family support under EIGRP was added.
12.2(18)S	This command was modified. Address family support under EIGRP was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2(33)SRB	This command was modified. Address family topology support under EIGRP was added.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX.
12.0(32)S12	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(24)T	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.3	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SXI1	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for asplain notation was added, and the default format for 4-byte autonomous system numbers is asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for asplain notation was added, and the default format for 4-byte autonomous system numbers is asplain.
15.0(1)M	This command was modified. The **nssa-only** keyword was added.
12.2(33)SRE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
15.1(1)SG	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
Cisco IOS XE Release 3.3SG	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers
Cisco IOS XE Release 3.9S	This command was modified. The **subnets** keyword was deprecated for OSPF classful redistribution.
15.2(1)E	This command was integrated into Cisco IOS Release 15.2(1)E.
Cisco IOS XE Release 3.12S	This command was modified. Support for redistribution of more than one application from one routing domain to another routing domain was added.
Cisco IOS XE Gibraltar 16.12.1x	Command is modified to include options for redistributing NHRP routes. The following keywords are added: **registered** , **resolved**, and **summary**.

Using the no Form of the redistribute Command

Caution Removing options that you have configured for the **redistribute** command requires careful use of the **no** form of the **redistribute** command to ensure that you obtain the result that you are expecting. Changing or disabling any keyword may or may not affect the state of other keywords, depending on the protocol.

It is important to understand that different protocols implement the **no** form of the **redistribute** command differently:

- In BGP, OSPF, and RIP configurations, the **no redistribute** command removes only the specified keywords from the **redistribute** commands in the running configuration. They use the *subtractive keyword* method when redistributing from other protocols. For example, in the case of BGP, if you configure **no redistribute static route-map interior**, *only the route map* is removed from the redistribution, leaving **redistribute static** in place with no filter.
    - An EIGRP routing process is configured when you issue the **router eigrp** command and then specify a network for the process using the **network** sub-command. Suppose that you have not configured an EIGRP routing process, and that you have configured redistribution of routes from such an EIGRP process into BGP, OSPF, or RIP. If you use the **no redistribute eigrp** command to change or disable a parameter in the **redistribute eigrp** command, the **no redistribute eigrp** command removes the entire **redistribute eigrp** command instead of changing or disabling a specific parameter.
- The **no redistribute isis** command removes the IS-IS redistribution from the running configuration. IS-IS removes the entire command, regardless of whether IS-IS is the redistributed or redistributing protocol.
- EIGRP used the subtractive keyword method prior to EIGRP component version rel5. Starting with EIGRP component version rel5, the **no redistribute** command removes the entire **redistribute** command when redistributing from any other protocol.

Additional Usage Guidelines for the redistribute Command

A router receiving a link-state protocol with an internal metric will consider the cost of the route from itself to the redistributing router plus the advertised cost to reach the destination. An external metric only considers the advertised metric to reach the destination.

Routes learned from IP routing protocols can be redistributed at Level 1 into an attached area or at Level 2. The **level-1-2** keyword allows both Level 1 and Level 2 routes in a single command.

Redistributed routing information must be filtered by the **distribute-list out** router configuration command. This guideline ensures that only those routes intended by the administrator are passed along to the receiving routing protocol.

Whenever you use the **redistribute** or the **default-information** router configuration commands to redistribute routes into an OSPF routing domain, the router automatically becomes an ASBR. However, an ASBR does not, by default, generate a default route into the OSPF routing domain.

When routes are redistributed into OSPF from protocols other than OSPF or BGP, and no metric has been specified with the **metric-type** keyword and *type-value* argument, OSPF will use 20 as the default metric. When routes are redistributed into OSPF from BGP, OSPF will use 1 as the default metric. When routes are redistributed from one OSPF process to another OSPF process, autonomous system external and not-so-stubby-area (NSSA) routes will use 20 as the default metric. When intra-area and inter-area routes are redistributed between OSPF processes, the internal OSPF metric from the redistribution source process is advertised as the external metric in the redistribution destination process. (This is the only case in which the routing table metric will be preserved when routes are redistributed into OSPF.)

When routes are redistributed into OSPF, only routes that are not subnetted are redistributed if the **subnets** keyword is not specified.

Note Depending on your release the **subnets**keyword is automatically appended when you use the **redistribute** *ospf* command. This automatic addition results in the redistribution of classless OSPF routes.

On a router internal to an NSSA area, the **nssa-only** keyword causes the originated type-7 NSSA LSAs to have their propagate (P) bit set to zero, which prevents area border routers from translating these LSAs into type-5 external LSAs. On an area border router that is connected to an NSSA and normal areas, the **nssa-only** keyword causes the routes to be redistributed only into the NSSA areas.

Routes configured with the **connected** keyword affected by this **redistribute** command are the routes not specified by the **network** router configuration command.

You cannot use the **default-metric** command to affect the metric used to advertise connected routes.

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

The default redistribution of Interior Gateway Protocol (IGP) or Exterior Gateway Protocol (EGP) into BGP is not allowed unless the **default-information originate** router configuration command is specified.

You can use the **redistribute nhrp** *process-id* [**metric** *metric-value*][**registered**] [**resolved**] [**summary**] [**route-map** *map-tag*] command to distribute all or specific NHRP routes. The routes that can be specified are registered, resolved, or summary routes. The keywords ‘registered’, ‘resolved’ and ‘summary’ are used to filter redistributed routes based on their origin. If none of these is specified, all NHRP routes are redistributed when redistribution from NHRP is configured.

Standard redistribution filtering mechanisms such as route-maps and tagging can also be used.

Release 12.2(33)SRB

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

4-Byte Autonomous System Number Support

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

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

Examples

The following example shows how OSPF routes are redistributed into a BGP domain:

```
Device(config)# router bgp 109
Device(config-router)# redistribute ospf
```

The following example shows how to redistribute EIGRP routes into an OSPF domain:

```
Device(config)# router ospf 110
Device(config-router)# redistribute eigrp
```

The following example shows how to redistribute the specified EIGRP process routes into an OSPF domain. The EIGRP-derived metric will be remapped to 100 and RIP routes to 200.

```
Device(config)# router ospf 109
Device(config-router)# redistribute eigrp 108 metric 100 subnets
Device(config-router)# redistribute rip metric 200 subnets
```

The following example shows how to configure BGP routes to be redistributed into IS-IS. The link-state cost is specified as 5, and the metric type is set to external, indicating that it has lower priority than internal metrics.

```
Device(config)# router isis
Device(config-router)# redistribute bgp 120 metric 5 metric-type external
```

The following example shows how to redistribute an application into an OSPF domain and specify a metric value of 5:

```
Device(config)# router ospf 4
Device(config-router)# redistribute application am metric 5
```

In the following example, network 172.16.0.0 will appear as an external LSA in OSPF 1 with a cost of 100 (the cost is preserved):

```
Device(config)# interface ethernet 0
Device(config-if)# ip address 172.16.0.1 255.0.0.0
Device(config-if)# exit
Device(config)# ip ospf cost 100
Device(config)# interface ethernet 1
Device(config-if)# ip address 10.0.0.1 255.0.0.0
!
Device(config)# router ospf 1
Device(config-router)# network 10.0.0.0 0.255.255.255 area 0
Device(config-if)# exit
Device(config-router)# redistribute ospf 2 subnet
Device(config)# router ospf 2
Device(config-router)# network 172.16.0.0 0.255.255.255 area 0
```

The following example shows how BGP routes are redistributed into OSPF and assigned the local 4-byte autonomous system number in asplain format. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, or a later release.

```
Device(config)# router ospf 2
Device(config-router)# redistribute bgp 65538
```

The following example shows how to remove the **connected metric 1000 subnets** options from the **redistribute connected metric 1000 subnets** command and leave the **redistribute connected** command in the configuration:

```
Device(config-router)# no redistribute connected metric 1000 subnets
```

The following example shows how to remove the **metric 1000** options from the **redistribute connected metric 1000 subnets** command and leave the **redistribute connected subnets** command in the configuration:

```
Device(config-router)# no redistribute connected metric 1000
```

The following example shows how to remove the **subnets** option from the **redistribute connected metric 1000 subnets** command and leave the **redistribute connected metric 1000** command in the configuration:

```
Device(config-router)# no redistribute connected subnets
```

The following example shows how to remove the **redistribute connected** command, and any of the options that were configured for the **redistribute connected** command, from the configuration:

```
Device(config-router)# no redistribute connected
```

The following example shows how EIGRP routes are redistributed into an EIGRP process in a named EIGRP configuration:

```
Device(config)# router eigrp virtual-name
Device(config-router)# address-family ipv4 autonomous-system 1
Device(config-router-af)# topology base
Device(config-router-af-topology)# redistribute eigrp 6473 metric 1 1 1 1 1
```

The following example shows how to set and disable the redistributions in EIGRP configuration. Note that, in the case of EIGRP, the **no** form of the commands removes the entire set of **redistribute** commands from the running configuration.

```
Device(config)# router eigrp 1
Device(config-router)# network 0.0.0.0
Device(config-router)# redistribute eigrp 2 route-map x
Device(config-router)# redistribute ospf 1 route-map x
Device(config-router)# redistribute bgp 1 route-map x
Device(config-router)# redistribute isis level-2 route-map x
Device(config-router)# redistribute rip route-map x

Device(config)# router eigrp 1
Device(config-router)# no redistribute eigrp 2 route-map x
Device(config-router)# no redistribute ospf 1 route-map x
Device(config-router)# no redistribute bgp 1 route-map x
Device(config-router)# no redistribute isis level-2 route-map x
Device(config-router)# no redistribute rip route-map x
Device(config-router)# end

Device# show running-config | section router eigrp 1

router eigrp 1
 network 0.0.0.0
```

The following example shows how to set and disable the redistributions in OSPF configuration. Note that the **no** form of the commands removes only the specified keywords from the **redistribute** command in the running configuration.

```
Device(config)# router ospf 1
Device(config-router)# network 0.0.0.0
Device(config-router)# redistribute eigrp 2 route-map x
Device(config-router)# redistribute ospf 1 route-map x
Device(config-router)# redistribute bgp 1 route-map x
Device(config-router)# redistribute isis level-2 route-map x
Device(config-router)# redistribute rip route-map x

Device(config)# router ospf 1
Device(config-router)# no redistribute eigrp 2 route-map x
Device(config-router)# no redistribute ospf 1 route-map x
Device(config-router)# no redistribute bgp 1 route-map x
Device(config-router)# no redistribute isis level-2 route-map x
Device(config-router)# no redistribute rip route-map x
Device(config-router)# end

Device# show running-config | section router ospf 1

router ospf 1
 redistribute eigrp 2
 redistribute ospf 1
 redistribute bgp 1
 redistribute rip
 network 0.0.0.0
```

The following example shows how to remove only the route map filter from the redistribution in BGP; redistribution itself remains in force without a filter:

```
Device(config)# router bgp 65000
Device(config-router)# no redistribute eigrp 2 route-map x
```

The following example shows how to remove the EIGRP redistribution to BGP:

```
Device(config)# router bgp 65000
Device(config-router)# no redistribute eigrp 2
```

The following example shows how registered NHRP routes are redistributed into a BGP domain:

```
Router(config)# router bgp 109
Router(config-router)# redistribute nhrp 11 registered
```

Related Commands

Command	Description
address-family (EIGRP)	Enters address family configuration mode to configure an EIGRP routing instance.
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
bgp asnotation dot	Changes the default display and the regular expression match format of BGP 4-byte autonomous system numbers from asplain (decimal values) to dot notation.

Command	Description
default-information originate (BGP)	Allows the redistribution of network 0.0.0.0 into BGP.
default-information originate (IS-IS)	Generates a default route into an IS-IS routing domain.
default-information originate (OSPF)	Generates a default route into an OSPF routing domain.
distribute-list out (IP)	Suppresses networks from being advertised in updates.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
router bgp	Configures the BGP routing process.
router eigrp	Configures the EIGRP address-family process.
show route-map	Displays all route maps configured or only the one specified.
topology (EIGRP)	Configures an EIGRP process to route IP traffic under the specified topology instance and enters address family topology configuration mode.

route-map

To define conditions for redistributing routes from one routing protocol to another routing protocol, or to enable policy routing, use the **route-map** command in global configuration mode. To delete an entry, use the **no** form of this command.

route-map *map-tag* [{**permit** | **deny**}] [*sequence-number*] **ordering-seq** *sequence-name*
no route-map *map-tag* [{**permit** | **deny**}] [*sequence-number*] **ordering-seq** *sequence-name*

Syntax Description

map-tag	Name for the route map.
permit	(Optional) Permits only routes matching the route map to be forwarded or redistributed.
deny	(Optional) Blocks routes matching the route map from being forwarded or redistributed.
sequence-number	(Optional) Number that indicates the position a new route map will have in the list of route maps already configured with the same name.
ordering-seq *sequence-name*	(Optional) Orders the route maps based on the string provided.

Command Default

Policy routing is not enabled and conditions for redistributing routes from one routing protocol to another routing protocol are not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.3(7)T	This command was updated for use in configuring IPv6 policy-based routing (PBR).
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE Release 2.1	This command was implemented on Cisco ASR 1000 Series Aggregation Services Routers.
12.2(33)SXI4	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SXI4.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
Cisco IOS XE Everest 16.6.1	The keyword **ordering-seq** was introduced in this release.

Usage Guidelines

Use the **route-map** command to enter route-map configuration mode.

Use route maps to redistribute routes or to subject packets to policy routing. Both purposes are described in this section.

Redistribution

Use the **route-map** global configuration command and the **match** and **set** route-map configuration commands to define the conditions for redistributing routes from one routing protocol to another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*--the conditions under which redistribution is allowed for the current **route-map**command. The **set** commands specify the *set actions*--the particular redistribution actions to be performed if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **match** route-map configuration command has multiple formats. The **match** commands can be given in any order, and all **match** commands must “pass” to cause the route to be redistributed according to the *set actions* given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

Use route maps when you want detailed control over how routes are redistributed between routing processes. The destination routing protocol is the one you specify with the **router** global configuration command. The source routing protocol is the one you specify with the **redistribute** router configuration command. See the “Examples” section for an illustration of how route maps are configured.

When you are passing routes through a route map, a route map can have several parts. Any route that does not match at least one **match** clause relating to a **route-map** command will be ignored; that is, the route will not be advertised for outbound route maps and will not be accepted for inbound route maps. If you want to modify only some data, you must configure a second route map section with an explicit match specified.

The **redistribute** router configuration command uses the name specified by the *map-tag* argument to reference a route map. Multiple route maps may share the same map tag name.

If the match criteria are met for this route map, and the **permit** keyword is specified, the route is redistributed as controlled by the set actions. In the case of policy routing, the packet is policy routed. If the match criteria are not met, and the **permit** keyword is specified, the next route map with the same map tag is tested. If a route passes none of the match criteria for the set of route maps sharing the same name, it is not redistributed by that set.

If the match criteria are met for the route map and the **deny** keyword is specified, the route is not redistributed. In the case of policy routing, the packet is not policy routed, and no further route maps sharing the same map tag name will be examined. If the packet is not policy routed, the normal forwarding algorithm is used.

Policy Routing

Another purpose of route maps is to enable policy routing. Use the **ip policy route-map** or **ipv6 policy route-map** command, in addition to the **route-map** command, and the **match** and **set** commands to define the conditions for policy routing packets. The **match** commands specify the conditions under which policy routing occurs. The **set** commands specify the routing actions to be performed if the criteria enforced by the **match** commands are met. You might want to policy route packets some way other than the obvious shortest path.

The *sequence-number* argument works as follows:

1. If no entry is defined with the supplied tag, an entry is created with the *sequence-number* argument set to 10.

2. If only one entry is defined with the supplied tag, that entry becomes the default entry for the following **route-map** command. The *sequence-number* argument of this entry is unchanged.

3. If more than one entry is defined with the supplied tag, an error message is printed to indicate that the *sequence-number* argument is required.

If the **no route-map** *map-tag* command is specified (with no *sequence-number* argument), the whole route map is deleted.

Examples

The following example shows how to redistribute Routing Information Protocol (RIP) routes with a hop count equal to 1 to Open Shortest Path First (OSPF). These routes will be redistributed to OSPF as external link-state advertisements (LSAs) with a metric of 5, metric type of Type 1, and a tag equal to 1.

```
Device(config)# router ospf 109
Device(config-router)# redistribute rip route-map rip-to-ospf
Device(config-router)# exit
Device(config)# route-map rip-to-ospf permit
Device(config-route-map)# match metric 1
Device(config-route-map)# set metric 5
Device(config-route-map)# set metric-type type1
Device(config-route-map)# set tag 1
```

The following example for IPv6 shows how to redistribute RIP routes with a hop count equal to 1 to OSPF. These routes will be redistributed into OSPF as external LSAs with a tag equal to 42 and a metric type equal to type1.

```
Device(config)# ipv6 router ospf 1
Device(config-router)# redistribute rip one route-map rip-to-ospfv3
Device(config-router)# exit
Device(config)# route-map rip-to-ospfv3
Device(config-route-map)# match tag 42
Device(config-route-map)# set metric-type type1
```

The following named configuration example shows how to redistribute Enhanced Interior Gateway Routing Protocol (EIGRP) addresses with a hop count equal to 1. These addresses are redistributed to EIGRP as external with a metric of 5 and a tag equal to 1:

```
Device(config)# router eigrp virtual-name1
Device(config-router)# address-family ipv4 autonomous-system 4453
Device(config-router-af)# topology base
Device(config-router-af-topology)# redistribute eigrp 6473 route-map
virtual-name1-to-virtual-name2
Device(config-router-af-topology)# exit-address-topology
Device(config-router-af)# exit-address-family
Device(config-router)# router eigrp virtual-name2
Device(config-router)# address-family ipv4 autonomous-system 6473
Device(config-router-af)# topology base
Device(config-router-af-topology)# exit-af-topology
Device(config-router-af)# exit-address-family
Device(config)# route-map virtual-name1-to-virtual-name2
Device(config-route-map)# match tag 42
Device(config-route-map)# set metric 5
Device(config-route-map)# set tag 1
```

Related Commands

Command	Description
ip policy route-map	Identifies a route map to use for policy routing on an interface.

Command	Description
ipv6 policy route-map	Configures IPv6 PBR on an interface.
match as-path	Matches a BGP autonomous system path access list.
match community	Matches a BGP community.
match interface (IP)	Distributes any routes that have their next hop on one of the specified interfaces.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match ipv6 address	Distributes IPv6 routes that have a prefix permitted by a prefix list or specifies an IPv6 access list to use to match packets for PBR for IPv6.
match ip next-hop	Redistributes any routes that have a next-hop router address passed by one of the specified access lists.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match length	Bases policy routing on the Level 3 length of a packet.
match metric (IP)	Redistributes routes with the metric specified.
match route-type (IP)	Redistributes routes of the specified type.
match tag	Redistributes routes in the routing table that match the specified tags.
router eigrp	Configures the EIGRP address-family process.
set as-path	Modifies an autonomous system path for BGP routes.
set automatic-tag	Automatically computes the tag value.
set community	Sets the BGP communities attribute.
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Indicates where to output packets that pass a match clause of a route map for policy routing.
set ipv6 default next-hop	Specifies an IPv6 default next hop to which matching packets will be forwarded.
set ip default next-hop verify-availability	Indicates where to output packets that pass a match clause of a route map for policy routing and for which the Cisco IOS software has no explicit route to a destination.

Command	Description
set ip next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing.
set ipv6 next-hop (PBR)	Indicates where to output IPv6 packets that pass a match clause of a route map for PBR for IPv6.
set level (IP)	Indicates where to import routes.
set local preference	Specifies a preference value for the autonomous system path.
set metric (BGP, OSPF, RIP)	Sets the metric value for a routing protocol.
set metric type	Sets the metric type for the destination routing protocol.
set next-hop	Specifies the address of the next hop.
set tag (IP)	Sets a tag value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.
show route-map	Displays all route maps configured or only the one specified.

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.
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.

Command	Description
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.

routing dynamic

To enable the router to pass routing updates to other routers through an interface, use the **routingdynamic**command in interface configuration mode. To disable the passing of routing updates through an interface, use the **no** form of this command.

routing dynamic
no routing dynamic

Syntax Description

This command has no arguments or keywords.

Command Default

Asynchronous interfaces: No routing updates are passed. All other interface types: Routing updates are passed.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(11)T	This command was introduced. This command replaces the **asyncdefaultrouting** command.

Usage Guidelines

Use the **routingdynamic**command to control the passing of routing updates over an interface.

Issuing the **noroutingdynamic**command flags the interface to indicate that routing updates should not be sent out of it.

The routing protocol must recognize the flag for this command to work as intended. The **routingdynamic**command sets and clears the flag; it does not enforce routing protocol conformance.

Examples

The following example enables routing over asynchronous interface 0:

```
interface async 0
 routing dynamic
```

The following example disables routing over serial interface 2/0:

```
interface serial 2/0
 no routing dynamic
```

Related Commands

Command	Description
async dynamic routing	Enables manually configured routing on an asynchronous interface.
passive-interface	Disables sending routing updates on an interface.