Cisco IOS IP Routing: Protocol-Independent Command Reference

C O N T E N T S

IP Routing Protocol-Independent Commands: A through R

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 commandaccept-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.
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.

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 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 multihop sessions, use the **authentication** command in BFD configuration mode. To disable authentication, use the **no** form of this command.

authentication *authentication-type* **keychain** *keychain-name*

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

Syntax Description

authentication-type	The authentication type. Valid values are: meticulous-md5, meticulous-sha-1, md5, and sha-1.
keychain *keychain-name*	(Required) Configures an authentication key chain. The maximum number of characters is 32.

Command Default

Authentication is not enabled.

Command Modes

BFD configuration (config-bfd)

Command History

Release	Modification
15.1(3)S	This command was introduced.

Usage Guidelines

You can configure authentication only in multihop templates. Although not required, authentication is recommended to enhance security. If used, authentication must be configured on each BFD source-destination pair and the authentication parameters must match on both ends.

Command Examples

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

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

Router(bfd-config)# 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.
12.4(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.

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

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)
- PoS
- Serial
- Tunnel (The tunnel type must be point-to-point, not Multiprotocol Label Switching (MPLS).

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.

Command Examples

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

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

Related Commands

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

bfd all-interfaces

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

> **bfd all-interfaces**
>
> **no bfd all-interfaces**

Syntax Description This command has no arguments or keywords.

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

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

Command History

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

Release	Modification
Cisco IOS XE Release 3.3	This command was modified. Support for the Routing Information Protocol was added.

Usage Guidelines

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

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

Command Examples

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

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

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

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

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

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

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

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

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

Router(config-router-af-interface)# **bfd**

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

```
Router> enable
```

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

Related Commands

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

bfd 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).

Command 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.

Command	Description
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.

Command 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 disable 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

The BFD map does not exist.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(3)S	This command was introduced.

Usage Guidelines

The **showbfdneighbors** command can be used to help troubleshoot the BFD feature.

The full output for the **details** keyword is not supported on the Route Processor (RP) for the Cisco 12000 series Internet router. If you want to enter the **showbfdneighbors** 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 **showbfdneighborsdetails** command will show the configured intervals, not the changed ones.

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

Usage Guidelines	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

Command Examples

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

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

Router(bfd-config)# interval min-tx 200 min-rx 200 multiplier 3
                    authentication sha-1 keychain bfd_multihop
                    exit
Router(config)# bfd
 map ipv4 10.11.11.0/24 10.36.42.5/32 vrf vpn1 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 2001:DB8::0:2::/64 vrf v6_1 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 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	Configures a BFD template.

Command	Description
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.

Command 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 create a Bidirectional Forwarding Detection (BFD) template and to enter BFD configuration mode, use the **bfd-template**command in global configuration mode. To disable 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	Specifies a single-hop BFD template.
multi-hop	Specifies a multi-hop BFD template.
template-name	The template name.

Command Default

The 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.

Usage Guidelines

The **bfd-template** command allows you to create a BFD template and places the router 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.

Cisco IOS Release 15.1(3)S and later releases support BFD on multiple network hops. The **bfd map** command associates the timers and authentication configured in the multihop templates with unique source-destination address pairs in multihop BFD sessions.

You can configure authentication only in multihop templates. Although it is not required, authentication is recommended to enhance security.

Command Examples

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

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

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

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

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

```
Router(bfd-config)# interval min-tx 200 min-rx 200 multiplier 3
                    authentication keyed-sha-1 keychain bfd_multihop
```

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 map	Configures a BFD map.
bfd slow-timer	Configures the BFD slow timer value.
interval	Configures the transmit and receive intervals between BFD packets.

dampening

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

dampening commanddampening [*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 20000 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

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.

Command 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-acl* | *ip-extended-acl* | *access-list-name*]

no distance *distance ip-address wildcard-mask* [*ip-standard-acl* | *ip-extended-acl* | *access-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.
ip-extended-acl	(Optional) Extended IP access list 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.

Release	Modification
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.

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.

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.

The **showipprotocols** 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.

Command Examples In the following example, the **routereigrp** 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.

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

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

```
Router> enable
Router# configure terminal
Router(config)# router eigrp 109
Router(config-router)# distance 22 10.0.0.0 0.0.0.255
Router(config-router)# distance 33 10.11.0.0 0.0.0.255
Router(config-router)# distance 44 10.11.12.0 0.0.0.255
Router(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 **showipprotocols** command displays the default administrative distance for the active routing processes, as well as the user-configured administrative distances:

```
Router# 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-listin** command in the appropriate configuration mode. To change or cancel the filter, use the **no** form of this command.

distribute-list [[*access-list-number* | *name*] | [**prefix** *prefix-name* | **gateway** *gateway-name* | [**route-map** *map-tag*]] **in** [*interface-type* | *interface-number*]

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

Syntax Description

access-list-number	*name*	(Optional) Standard IP access list number or name. The list defines which networks are to be received and which are to be suppressed in routing updates.
prefix *prefix-name*	(Optional) Filters prefixes in address updates.
gateway *gateway-name*	(Optional) Filters incoming address updates based on gateway.
route-map *map-tag*	(Optional) Name of 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. This argument is supported by OSPF and EIGRP.
interface-type	(Optional) Interface type. 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 can apply if you specify an access list, not a route map. The *interface-number*argument cannot be used in address-family configuration mode.

Command Default   Networks received in updates are not filtered.

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*, *type*, and *number* arguments were added.
	12.0(7)T	Address-family configuration mode was added.
	12.0(24)S	The **route-map***map-tag* keyword and argument were 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	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

This command must specify either an access list or a map-tag name of a route map. The route map is supported for OSPF and 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.

Command 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:

```
Router(config)# access-list 1 permit 0.0.0.0
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 eigrp 1

Router(config-router)# network 10.108.0.0
Router(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:

```
Router(config)# access-list 1 permit 0.0.0.0
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 eigrp virtual-name

Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# network 10.108.0.0
Router(config-router-af)# network 10.0.0.0
Router(config-router-af)# topology base
Router(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.

```
Router(config)# route-map tag-filter deny 10
Router(config-route-map)# match tag 777

Router(config-route-map)# route-map tag-filter permit 20

Router(config-route-map)# exit
Router(config)# router eigrp virtual-name

Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# network 10.108.0.0
Router(config-router-af)# network 10.0.0.0
Router(config-router-af)# topology base
Router(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.

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

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
access-list (IP standard)	Defines a standard IP access list.
distribute-list out (IP)	Suppresses networks from being advertised in updates.
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-number* | *access-list-name*} **out** [*interface-name* | *routing-process* | *as-number*]

> **no distribute-list** {*access-list-number* | *access-list-name*} **out** [*interface-name* | *routing-process* | *as-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.

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

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-list in** command.

Release 12.2(33)SRB

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

Command 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.
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.

Command 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.

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.

Command 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.

Command 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.

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 iThis command was modified. The **microseconds** keyword was added. ntroduced.

Usage Guidelines

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

Command 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.

Command 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.

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.

Command 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.
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 **ippolicyroute-map** command in interface configuration mode. Todisable policy routing on the interface, use the **no**form of this command.

ip policy route-map commandip 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

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 **ippolicyroute-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 *matchcriteria*--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 **noippolicyroute-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**matchipaddress**command and referencing an extended IP access list.

Command 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. Toremove static routes, use the **no**form of this command.

> **ip route command ip route** [**vrf** *vrf-name*] *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]} [**dhcp**] [*distance*] [**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**] [*distance*] [**name** *next-hop-name*] [**permanent** | **track** *number*] [**tag** *tag*]

Syntax Description

vrf *vrf-name*	(Optional) Configures the name of the VRF by which static routes should be specified.
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.
distance	(Optional) Administrative distance. 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.

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.

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.

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 **redistributestatic** 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 **redistributestatic**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**iproute**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 **redistributestatic**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 **iproute0.0.0.00.0.0.0ethernet1/2** 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 **iproute0.0.0.00.0.0.0ethernet1/2**,displays a warning message. 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.

Command 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 **showrunning-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
```

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.

> **iip 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.

Command 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.

Command 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 **iproutestaticbfd**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* [**group** *group-name* [**passive**]]

> **no ip route static bfd** {*interface-type interface-number ip-address* [**group** *group-name* [**passive**]] | **group** *group-name*}

Syntax Description

interface-type interface-number	Interface type and number.
ip-address	IP address of the gateway, in A.B.C.D format.
group *group-name*	(Optional) Assigns a BFD group. Character string of up to 32 characters specifying the BFD group name.
passive	(Optional) Specifies the passive member of the group.

Command Default

No static 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 modified. The **group***group-name* keyword-argument pair and the **passive** keyword were added.

Usage Guidelines

Use the **iproutestaticbfdcommandtospecifystaticrouteBFDneighbors.Allstaticroutesthathavethesameinterface andgatewayspecifiedintheconfigurationsharethesameBFDsessionforreachabilitynotification.**

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 and 15.1(2)S releases.

The **group**keywordassigns 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 a static BFD in a group without the **passive** keyword makes it 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 **noiproutestaticbfd** command and specify the BFD group name.

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

Command Examples

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

```
Router# configure terminal
```

Router(config) #**iproutestaticbfdGigabitEthernet1/110.1.1.1groupgroup1**

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

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

Related Commands

Command	Description
debug ip routing static bfd	Enables debugging output on IP static BFD neighbor events.
show ip static route	Displays static route database information.

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.

Command 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.

Command 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
```

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 commandkey *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.

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 commandkey chain** *name-of-chain*
>
> **no key chain** *name-of-chain*

Syntax Description

name-of-chain	Name of a key chain. A key chain must have at least one key and can have up to 2147483647 keys.

Command Default   No key chain exists.

Command Modes   Global configuration (config)

Command History

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

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

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

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

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

```
Router(config)# router eigrp virtual-name
Router(config-router)# service-family ipv4 autonomous-system 4453
Router(config-router-sf)# sf-interface ethernet
Router(config-router-sf-interface)# authentication key chain trees
Router(config-router-sf-interface)# authentication mode md5
Router(config-router-sf-interface)# exit
Router(config-router-sf)# exit
Router(config-router)# exit
Router(config)# key chain chain1
Router(config-keychain)# key 1
```

```
Router(config-keychain-key)# key-string chestnut
Router(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 14:00:00 Jan 25 1996 duration 3600
Router(config-keychain-key)# exit
Router(config-keychain)# key 2
Router(config-keychain-key)# key-string birch
Router(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 15:00:00 Jan 25 1996 duration 3600
```

Related Commands

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

key-string (authentication)

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

key-string commandkey-string *text*

no key-string *text*

Syntax Description

text	Authentication string that must be sent and received in the packets using the routing protocol being authenticated. The string can contain from 1 to 80 uppercase and lowercase alphanumeric characters, except that the first character cannot be a number.

Command Default No authentication string for a key exists.

Command Modes Key chain key configuration (config-keychain-key)

Command History

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

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

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

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 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.

Command	Description
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.

Command 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.

Command	Description
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.

Release	Modification
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.

Command 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.

Command	Description
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.
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-number* | *access-list-name*} [... *access-list-number* | ... *access-list-name*]

> **no match ip next-hop** {*access-list-number* | *access-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-number*or*access-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.

Command 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.

Command	Description
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.

Command 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.

Command	Description
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 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.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	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 **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.

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.

Command 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.

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 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.
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 length

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

match length commandmatch length *minimum-length maximum-length*

no match length *minimum-length maximum-length*

Syntax Description

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

Command Default

No policy routing occurs on the length of a packet.

Command Modes

Route-map configuration

Command History

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

Usage Guidelines

In IPv4, use the **ippolicyroute-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 **ippolicyroute-map** command identifies a route map by name. Each **route-map** has a list of **match** and **set** commands associated with it. The **match** commands specify the *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.

In PBR for IPv6, use the **ipv6policyroute-map**or **ipv6localpolicyroute-map**command to define conditions for policy routing packets.

In IPv4, the **match** route-map configuration command has multiple formats. The **match** commands can be given in any order, and all **match** commands must "pass" to cause the packet to be routed according to the *setactions*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.

Command Examples

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

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

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

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

Related Commands

Command	Description
ip local policy route-map	Identifies a route map to use for policy routing on an interface.
ipv6 local policy route-map	Configures PBR for IPv6 for originated packets.
ipv6 policy route-map	Configures IPv6 PBR on an interface.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match ipv6 address	Specifies an IPv6 access list to use to match packets for PBR for IPv6.
match length	Bases policy routing on the Level 3 length of a packet.

Command	Description
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Indicates where to output packets that pass a match clause of route map for policy routing.
set ip default next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing and for which the Cisco IOS software has no explicit route to a destination.
set ipv6 default next-hop	Specifies an IPv6 default next hop to which matching packets will be forwarded.
set ip next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing.
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).

Command 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.

Command	Description
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.
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.

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

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.

Command 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.

Command	Description
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 redistribute routes in the routing table that match the specified tags, use the **matchtag**command in route-map configuration mode. To remove the tag entry, use the **no** form of this command.

> **match tag** *tag-value* [... *tag-value*]
>
> **no match tag** *tag-value* [... *tag-value*]

Syntax Description

tag-value	List of one or more route tag values. Each can be an integer from 0 to 4294967295.

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.

Usage Guidelines

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *tag-value* 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.

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.

Command Examples

The following example redistributes routes stored in the routing table with tag 5:

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

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 route-type (IP)	Redistributes routes of the specified type.
route-map	Defines the conditions for redistributing routes from one routing protocol into another.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.

Command	Description
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.

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

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 made available in router address family topology configuration mode.
12.2(33)SXH	The maximum number of paths was changed from 8 to 16 for Cisco IOS Release 12.2(33)SXH.

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 in order for this OSPF router configuration command to become topology-aware.

Command Examples

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

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

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.

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 abort 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.

Command 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 .

Command 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 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.

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 .

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

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

redistribute (IP)

To redistribute routes from one routing domain into another routing domain, use the **redistribute** command in the appropriate configuration mode. To disable redistribution, use the **no** form of this command.

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*] [**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*] [**subnets**] [**nssa-only**]

Syntax Description		
protocol		Source protocol from which routes are being redistributed. It can be one of the following keywords:**bgp**, **connected**, **eigrp**,**isis**, **mobile**, **ospf**,**static** [**ip**], or **rip**.
		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 **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 **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. You can specify only one IS-IS process per router. Creating a name for a routing process means that you use names when configuring routing.
		For the **ospf**keyword, 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 **rip**keyword, no *process-id* value is needed.
		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 **routerbgp** 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.
metric transparent	(Optional) Causes Routing Information Protocol (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 route. • **external 2** --Routes that are external to the autonomous system, but are imported into OSPF as Type 2 external route. The default is **internal** and **external 1**.
tag *tag-value*	(Optional) Specifies the 32-bit decimal value attached to each external route. This is not used by OSPF itself. It may be used to communicate information between Autonomous System Boundary Routers (ASBRs). If none is specified, then the remote autonomous system number is used for routes from Border Gateway Protocol (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.

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.
12.2(33)SRB	This command was modified. This command was made available in router address family topology configuration mode.
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.

Release	Modification
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.

Usage Guidelines

Changing or disabling any keyword will not affect the state of other keywords.

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-listout** 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 *defaultroute* 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.

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 a 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 using 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.

Using the no Form of the redistribute Command

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. See the "Examples" section for more information.

Release 12.2(33)SRB

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

Command Examples   The following example shows how OSPF routes are redistributed into a BGP domain:

```
Router(config)# router bgp 109
Router(config-router)# redistribute ospf
```

The following example shows how to redistribute EIGRP routes into an OSPF domain:

```
Router(config)# router ospf 110
Router(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.

```
Router(config)# router ospf 109
Router(config-router)# redistribute eigrp 108 metric 100 subnets
Router(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.

```
Router(config)# router isis
Router(config-router)# redistribute bgp 120 metric 5 metric-type external
```

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):

```
Router(config)# interface ethernet 0
Router(config-if)# ip address 172.16.0.1 255.0.0.0
Router(config)# ip ospf cost 100
Router(config)# interface ethernet 1
Router(config-if)# ip address 10.0.0.1 255.0.0.0
!
Router(config)# router ospf 1
Router(config-router)# network 10.0.0.0 0.255.255.255 area 0
Router(config-router)# redistribute ospf 2 subnet
Router(config)# router ospf 2
Router(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.

```
Router(config)# router ospf 2
Router(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:

```
Router(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:

```
Router(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:

```
Router(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:

```
Router(config-router)# no redistribute connected
```

The following example shows how EIGRP routes are redistributed into an EIGRP process in a named EIGRP configuration:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 1
```

```
Router(config-router-af)# topology base
Router(config-router-af-topology)# 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 the **no** form of the commands removes the entire set of **redistribute** commands from the running configuration.

```
Router(config)# router eigrp 1
Router(config-router)# network 0.0.0.0
Router(config-router)# redistribute eigrp 2 route-map x
Router(config-router)# redistribute ospf 1 route-map x
Router(config-router)# redistribute bgp 1 route-map x
Router(config-router)# redistribute isis level-2 route-map x
Router(config-router)# redistribute rip route-map x

Router(config)# router eigrp 1
Router(config-router)# no redistribute eigrp 2 route-map x
Router(config-router)# no redistribute ospf 1 route-map x
Router(config-router)# no redistribute bgp 1 route-map x
Router(config-router)# no redistribute isis level-2 route-map x
Router(config-router)# no redistribute rip route-map x
Router(config-router)# end

Router# 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.

```
Router(config)# router ospf 1
Router(config-router)# network 0.0.0.0
Router(config-router)# redistribute eigrp 2 route-map x
Router(config-router)# redistribute ospf 1 route-map x
Router(config-router)# redistribute bgp 1 route-map x
Router(config-router)# redistribute isis level-2 route-map x
Router(config-router)# redistribute rip route-map x

Router(config)# router ospf 1
Router(config-router)# no redistribute eigrp 2 route-map x
Router(config-router)# no redistribute ospf 1 route-map x
Router(config-router)# no redistribute bgp 1 route-map x
Router(config-router)# no redistribute isis level-2 route-map x
Router(config-router)# no redistribute rip route-map x
Router(config-router)# end

Router# 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
```

In BGP and RIP configurations, the **no redistribute** command removes only the specified keywords from the **redistribute** commands in the running configuration. An exception to this is the **redistribute isis** command, which is entirely removed from the running configuration.

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.
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 the conditions for redistributing routes from one routing protocol into another routing protocol, or to enable policy routing, use the **route-map** command in global configuration mode and the **match** and **set** commands in route-map configuration modes. To delete an entry, use the **no**form of this command.

> **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]

> **no route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]

Syntax Description

map-tag	A meaningful name for the route map. The **redistribute** router configuration command uses this name to reference this route map. Multiple route maps may share the same map tag name.
permit	(Optional) If the match criteria are met for this route map, and the **permit** keyword is specified, the route is redistributed as controlled by the set actions. In the case of policy routing, the packet is policy routed.
	If the match criteria are not met, and the **permit** keyword is specified, the next route map with the same map tag is tested. If a route passes none of the match criteria for the set of route maps sharing the same name, it is not redistributed by that set.
deny	(Optional) If the match criteria are met for the route map and the **deny** keyword is specified, the route is not redistributed. In the case of policy routing, the packet is not policy routed, and no further route maps sharing the same map tag name will be examined. If the packet is not policy routed, the normal forwarding algorithm is used.
sequence-number	(Optional) Number that indicates the position a new route map will have in the list of route maps already configured with the same name. If used with the **no** form of this command, the position of the route map should be deleted.

Command Default

Policy routing is not enabled and conditions for redistributing routes from one routing protocol into another routing protocol are not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.3(7)T	This command was updated for use in configuring IPv6 policy-based routing (PBR).
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE Release 2.1	This command was implemented on Cisco ASR 1000 Series Aggregation Services Routers.
12.2(33)SXI4	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SXI4.

Usage Guidelines

Use the **route-map** command to enter route-map configuration mode.

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

Redistribution

Use the **route-map** global configuration command, and the **match** and **set** route-map configuration commands, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *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.

Use route maps when you want detailed control over how routes are redistributed between routing processes. The destination routing protocol is the one you specify with the **router** global configuration command. The source routing protocol is the one you specify with the **redistribute** router configuration command. See the "Examples" section for an illustration of how route maps are configured.

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

Policy Routing

Another purpose of route maps is to enable policy routing. Use the ip policy route-map or **ipv6policyroute-map**command, in addition to the **route-map** command, and the **match** and **set** commands to define the conditions for policy routing packets. The **match** commands specify the conditions under which policy routing occurs. The **set** commands specify the routing actions to perform if the criteria enforced by the

match commands are met. You might want to policy route packets some way other than the obvious shortest path.

The *sequence-number* argument works as follows:

1 If no entry is defined with the supplied tag, an entry is created with the *sequence-number* argument set to 10.
2 If only one entry is defined with the supplied tag, that entry becomes the default entry for the following **route-map** command. The *sequence-number*argumentof 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 **noroute-map***map-tag* command is specified (with no *sequence-number*argument), the whole route map is deleted.

Command Examples

The following example redistributes Routing Information Protocol (RIP) routes with a hop count equal to 1 into Open Shortest Path First (OSPF). These routes will be redistributed into OSPF as external link-state advertisements (LSAs) with a metric of 5, metric type of Type 1, and a tag equal to 1.

```
Router(config)# router ospf 109
Router(config-router)# redistribute rip route-map rip-to-ospf
Router(config-router)# exit
Router(config)# route-map rip-to-ospf permit
Router(config-route-map)# match metric 1
Router(config-route-map)# set metric 5
Router(config-route-map)# set metric-type type1
Router(config-route-map)# set tag 1
```

The following example for IPv6 redistributes RIP routes with a hop count equal to 1 into OSPF. These routes will be redistributed into OSPF as external LSAs with a tag equal to 42 and a metric type equal to type1.

```
Router(config)# ipv6 router ospf 1
Router(config-router)# redistribute rip one route-map rip-to-ospfv3
Router(config-router)# exit
Router(config)# route-map rip-to-ospfv3
Router(config-route-map)# match tag 42
Router(config-route-map)# set metric-type type1
```

The following named configuration example redistributes Enhanced Interior Gateway Routing Protocol (EIGRP) addresses with a hop count equal to 1. These addresses are redistributed into EIGRP as external with a metric of 5 and a tag equal to 1:

```
Router(config)# router eigrp virtual-name1
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# topology base
Router(config-router-af-topology)# redistribute eigrp 6473 route-map virtual-name1-to-
virtual-name2
Router(config-router-af-topology)# exit-address-topology
Router(config-router-af)# exit-address-family
Router(config-router)# router eigrp virtual-name2
Router(config-router)# address-family ipv4 autonomous-system 6473
Router(config-router-af)# topology base
Router(config-router-af-topology)# exit-af-topology
Router(config-router-af)# exit-address-family
Router(config)# route-map virtual-name1-to-virtual-name2
Router(config-route-map)# match tag 42
Router(config-route-map)# set metric 5
Router(config-route-map)# set tag 1
```

Related Commands

Command	Description
ip policy route-map	Identifies a route map to use for policy routing on an interface.
ipv6 policy route-map	Configures IPv6 PBR on an interface.
match as-path	Matches a BGP autonomous system path access list.
match community	Matches a BGP community.
match interface (IP)	Distributes any routes that have their next hop out one of the interfaces specified.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match ipv6 address	Distributes IPv6 routes that have a prefix permitted by a prefix list or to specify an IPv6 access list to use to match packets for PBR for IPv6.
match ip next-hop	Redistributes any routes that have a next hop router address passed by one of the access lists specified.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match length	Bases policy routing on the Level 3 length of a packet.
match metric (IP)	Redistributes routes with the metric specified.
match route-type (IP)	Redistributes routes of the specified type.
match tag	Redistributes routes in the routing table that match the specified tags.
router eigrp	Configures the EIGRP address-family process.
set as-path	Modifies an autonomous system path for BGP routes.
set automatic-tag	Automatically computes the tag value.
set community	Sets the BGP communities attribute.
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.

Command	Description
set interface	Indicates where to output packets that pass a match clause of a route map for policy routing.
set ipv6 default next-hop	Specifies an IPv6 default next hop to which matching packets will be forwarded.
set ip default next-hop verify-availability	Indicates where to output packets that pass a match clause of a route map for policy routing and for which the Cisco IOS software has no explicit route to a destination.
set ip next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing.
set ipv6 next-hop (PBR)	Indicates where to output IPv6 packets that pass a match clause of a route map for PBR for IPv6.
set level (IP)	Indicates where to import routes.
set local preference	Specifies a preference value for the autonomous system path.
set metric (BGP, OSPF, RIP)	Sets the metric value for a routing protocol.
set metric type	Sets the metric type for the destination routing protocol.
set next-hop	Specifies the address of the next hop.
set tag (IP)	Sets a tag value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.
show route-map	Displays all route maps configured or only the one specified.

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.

Command 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.

IP Routing Protocol-Independent Commands: S through T

send-lifetime

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

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

no send-lifetime *start-time* {**infinite** | *end-time* | **duration** *seconds*}

Syntax Description

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

Command Default

Forever (the starting time is January 1, 1993, and the ending time is infinite)

Command Modes

Key chain key configuration (config-keychain-key)

Command History

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

Usage Guidelines

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

We recommend running Network Time Protocol (NTP) or some other time synchronization method if you intend to set lifetimes on keys.

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

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

```
Router(config)# eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# network 10.0.0.0
```

```
Router(config-router-af)# af-interface ethernet0/0
Router(config-router-af-interface)# authentication key-chain trees
Router(config-router-af-interface)# authentication mode md5
Router(config-router-af-interface)# exit
Router(config-router-af)# exit
Router(config-router)# exit
Router(config)# key chain chain1
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string key1
Router(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 14:00:00 Jan 25 1996 duration 3600
Router(config-keychain-key)# exit
Router(config-keychain)# key 2
Router(config-keychain-key)# key-string key2
Router(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 15:00:00 Jan 25 1996 duration 3600
```

Related Commands

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

set automatic-tag

To automatically compute the tag value, use the **setautomatic-tag** command in route-map configuration mode. To disable this function, use the **no** form of this command.

set automatic-tag commandset automatic-tag

no set automatic-tag

Syntax Description   This command has no arguments or keywords.

Command Default   This command is disabled by default.

Command Modes   Route-map configuration

Command History

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

Usage Guidelines   You must have a match clause (even if it points to a "permit everything" list) if you want to set tags.

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 **set** route-map configuration commands specify the redistribution *setactions* to be performed when all the match criteria of a route map are met. When all match criteria are met, all set actions are performed.

Command Examples   The following example configures the Cisco IOS software to automatically compute the tag value for the Border Gateway Protocol (BGP) learned routes:

```
route-map tag
 match as path 10
 set automatic-tag
!
router bgp 100
 table-map tag
```

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 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 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.

Command	Description
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.

set default interface

To indicate where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination, use the **setdefaultinterface** command in route-map configuration mode. To delete an entry, use the **no** form of this command.

> **set default interface** *type number* [... *type number*]

> **no set default interface** *type number* [... *type number*]

Syntax Description

type	Interface type, used with the interface number, to which packets are output.
number	Interface number, used with the interface type, to which packets are output.

Command Default

This command is disabled by default.

Command Modes

Route-map configuration

Command History

Release	Modification
11.0	This command was introduced.
12.3(7)T	This command was updated for use in configuring IPv6 policy-based routing (PBR).
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)S.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.2S	This command was modified. It was integrated into Cisco IOS XE Release 3.2S.

Usage Guidelines

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

Use this command to provide certain users a different default route. If the Cisco IOS software has no explicit route for the destination, then it routes the packet to this interface. The first interface specified with the **setdefaultinterface** command that is up is used. The optionally specified interfaces are tried in turn.

Use the **ippolicyroute-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 **ippolicyroute-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 **ipv6policyroute-map**or **ipv6localpolicyroute-map**command with match and set route map configuration commands to define conditions for policy routing packets.

The set clauses can be used in conjunction with one another. They are evaluated in the following order:

1 **set ip next-hop**
2 **set interface**
3 **set ip default next-hop**
4 **set default interface**

Command Examples

In the following example, packets that have a Level 3 length of 3 to 50 bytes and for which the software has no explicit route to the destination are output to Ethernet interface 0:

```
interface serial 0
 ip policy route-map brighton
!
route-map brighton
 match length 3 50
 set default interface ethernet 0
```

Related Commands

Command	Description
ip policy route-map	Identifies a route map to use for policy routing on an interface.
ipv6 local policy route-map	Identifies a route map to use for local IPv6 PBR.
ipv6 policy route-map	Configures IPv6 PBR on an interface.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match ipv6 address	Specifies an IPv6 access list to use to match packets for PBR for IPv6.
match length	Bases policy routing on the Level 3 length of a packet.

Command	Description
route-map	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Indicates where to output packets that pass a match clause of route map for policy routing.
set ip default next-hop verify-availability	Indicates where to output packets that pass a match clause of a route map for policy routing and for which the Cisco IOS software has no explicit route to a destination.
set ipv6 default next-hop	Specifies an IPv6 default next hop to which matching packets will be forwarded.
set ip next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing.
set ipv6 next-hop (PBR)	Indicates where to output IPv6 packets that pass a match clause of a route map for policy routing.
set ipv6 precedence	Sets the precedence value in the IPv6 packet header.

set interface

To indicate where to forward packets that pass a match clause of a route map for policy routing, use the **setinterface**command in route-map configuration mode. To delete an entry, use the **no** form of this command.

>   **set interface** *type number* [... *type number*]

>   **no set interface** *type number* [... *type number*]

Syntax Description

type	Interface type, used with the interface number, to which packets are forwarded.
number	Interface number, used with the interface type, to which packets are forwarded.

Command Default   Packets that pass a match clause are not forwarded to an interface.

Command Modes   Route-map configuration (config-route-map)

Command History

Release	Modification
11.0	This command was introduced.
12.3(7)T	This command was updated for use in configuring IPv6 policy-based routing (PBR).
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB, and hardware switching support was introduced for the Cisco 7600 series platform.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.2S	This command was modified. It was integrated into Cisco IOS XE Release 3.2S.

Usage Guidelines	An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *type*and*number* arguments .

Use the**ippolicyroute-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 **ippolicyroute-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 *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.

In PBR for IPv6, use the **ipv6policyroute-map**or **ipv6localpolicyroute-map**command with **match** and **set** route-map configuration commands to define conditions for policy-routing packets.

If the first interface specified with the **setinterface** command is down, the optionally specified interfaces are tried in turn.

The **set** clauses can be used in conjunction with one another. They are evaluated in the following order:

1 **set ip next-hop**
2 **set interface**
3 **set ip default next-hop**
4 **set default interface**

A useful next hop implies an interface. As soon as a next hop and an interface are found, the packet is routed.

Specifying the **setinterfacenull0** command is a way to write a policy that the packet be dropped and an "unreachable" message be generated. In Cisco IOS Release 12.4(15)T and later releases, the packets are dropped; however, the "unreachable" messages are generated only when CEF is disabled.

In Cisco IOS Release 12.2(33)SRB and later releases, hardware switching support was introduced for PBR packets sent over a traffic engineering (TE) tunnel interface on a Cisco 7600 series router. When a TE tunnel interface is configured using the **setinterface** command in a policy, the packets are processed in hardware. In previous releases, PBR packets sent over TE tunnels are fast switched by Route Processor software.

Command Examples	In the following example, packets with a Level 3 length of 3 to 50 bytes are forwarded to Ethernet interface 0:

```
interface serial 0
 ip policy route-map testing
!
route-map testing
 match length 3 50
 set interface ethernet 0
```

In the following example for IPv6, packets with a Level 3 length of 3 to 50 bytes are forwarded to Ethernet interface 0:

```
interface serial 0
 ipv6 policy route-map testing
!
route-map testing
 match length 3 50
 set interface ethernet 0
```

In the following example, a TE tunnel interface is configured on a Cisco 7600 series router using the **setinterface** command in a policy, and the packets are processed in hardware, instead of being fast

switched by Route Processor software. This example can be used only with a Cisco IOS Release 12.2(33)SRB, or later release, image.

```
interface Tunnel101
 description FRR-Primary-Tunnel
 ip unnumbered Loopback0
 tunnel destination 172.17.2.2
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng path-option 1 explicit name p1
!
access-list 101 permit ip 10.100.0.0 0.255.255.255 any
!
route-map test permit 10
 match ip address 101
 set interface Tunnel101
!
interface GigabitEthernet9/5
 description TO_CE_C1A_FastEther-5/5
 ip address 192.168.5.1 255.255.255.0
 ip policy route-map test
 no keepalive
```

Related Commands

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

Command	Description
set ip next-hop	Indicates where to forward packets that pass a match clause of a route map for policy routing.
set ipv6 default next-hop	Specifies an IPv6 default next hop to which matching packets will be forwarded.
set ipv6 next-hop (PBR)	Indicates where to output IPv6 packets that pass a match clause of a route map for policy routing.
set ipv6 precedence	Sets the precedence value in the IPv6 packet header.

set ip default next-hop

To indicate 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, use the **setipdefaultnext-hop** command in route-map configuration mode. To delete an entry, use the **no** form of this command.

> **set ip default next-hop** *ip-address* [... *ip-address*]
>
> **no set ip default next-hop** *ip-address* [... *ip-address*]

Syntax Description

ip-address	IP address of the next hop to which packets are output.The next hop must be an adjacent router.

Command Default

This command is disabled by default.

Command Modes

Route-map configuration

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.

Usage Guidelines

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *ip-address* argument .

Use this command to provide certain users a different default route. If the software has no explicit route for the destination in the packet, then it routes the packet to this next hop. The first next hop specified with the **setipdefaultnext-hop**command needs to be adjacent to the router. The optional specified IP addresses are tried in turn.

Use the ip policy route-map interface configuration command, the **route-map** global configuration command, and the **match** and **set** route-map configuration commands to define the conditions for policy routing packets. The **ippolicyroute-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 *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.

The set clauses can be used in conjunction with one another. They are evaluated in the following order:

1. **set ip next-hop**
2. **set interface**
3. **set ip default next-hop**
4. **set default interface**

Note The set ip next-hop and set ip default next-hop are similar commands but have a different order of operations. Configuring the set ip next-hop command causes the system to use policy routing first and then use the routing table. Configuring the set ip default next-hop command causes the system to use the routing table first and then policy route the specified next hop.

Command Examples The following example provides two sources with equal access to two different service providers. Packets arriving on asynchronous interface 1 from the source 10.1.1.1 are sent to the router at 172.16.6.6 if the software has no explicit route for the destination of the packet. Packets arriving from the source 10.2.2.2 are sent to the router at 172.17.7.7 if the software has no explicit route for the destination of the packet. All other packets for which the software has no explicit route to the destination are discarded.

```
access-list 1 permit ip 10.1.1.1 0.0.0.0
access-list 2 permit ip 10.2.2.2 0.0.0.0
!
interface async 1
 ip policy route-map equal-access
!
route-map equal-access permit 10
 match ip address 1
 set ip default next-hop 172.16.6.6
route-map equal-access permit 20
 match ip address 2
 set ip default next-hop 172.17.7.7
 route-map equal-access permit 30
 set default interface null0
```

Related Commands

Command	Description
ip policy route-map	Identifies a route map to use for policy routing on an interface.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match length	Bases policy routing on the Level 3 length of a packet.

Command	Description
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 next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing.

set ip default next-hop verify-availability

To configure a router, for policy routing, to check the CDP database for the availability of an entry for the default next hop that is specified by the set ip default next-hop command, use the set ip default next-hop verify-availability route map configuration command. To disable this function, use the **no** form of this command.

> set ip default next-hop commandset ip default next-hop verify-availability
>
> no set ip default next-hop verify-availability

Syntax Description   This command has no arguments or keywords.

Command Default   This command is disabled by default.

Command Modes   Route-map configuration

Command History

Release	Modification
12.1(1.05)T	This command was introduced.

Usage Guidelines   Use this command to force the configured policy routing to check the CDP database to determine if an entry is available for the next hop that is specified by the set ip default next-hop command. This command is used to prevent traffic from being "black holed" if the configured next hop becomes unavailable.

Command Examples   The following example:

```
Router(config-route-map)# set ip default next-hop verify-availability
```

Related Commands

Command	Description
set ip default next-hop verify-availability	Configures policy routing to verify if the next hops of a route map are CDP neighbors before policy routing to those next hops.
set ip next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing.

set ip global

To indicate where to forward packets that pass a match clause of a route map for policy routing and for which the Cisco IOS software uses the global routing table, use the **setipglobal**command in route-map configuration mode. To disable this feature, use the **no** form of this command.

> **set ip global next-hop** *ip-address* [... *ip-address*]
>
> **no set ip global next-hop** *ip-address* [... *ip-address*]

Syntax Description

next-hop *ip-address*	IP address of the next hop.

Command Default

The router uses the next-hop address in the global routing table.

Command Modes

Route-map configuration

Command History

Release	Modification
12.2(33)SRB1	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

Use this command to allow packets to enter a VRF interface and be policy-routed or forwarded out of the global table.

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *ip-address* argument.

Command Examples

The following example allows use of the global table and specifies that the next-hop address is 10.5.5.5:

```
set ip global next-hop 10.5.5.5
```

Related Commands

Command	Description
ip policy route-map	Identifies a route map to use for policy routing on an interface.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match length	Bases policy routing on the Level 3 length of a packet.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Indicates where to output packets that pass a match clause of 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 vrf	Indicates where to forward packets that pass a match clause of a route map for policy routing when the next hop must be under a specified VRF name.

set ip next-hop

To indicate where to output packets that pass a match clause of a route map for policy routing, use the **setipnext-hop** command in route-map configuration mode. To delete an entry, use the **no** form of this command.

set ip next-hop {*ip-address* [**...***ip-address*] | **dynamic dhcp** | **encapsulate l3vpn** *profile name* | **peer-address** | **recursive** [**global** | **vrf** *vrf name*] *ip-address* | **verify-availability** [*ip-address sequence* **track** *track object number*}

no set ip next-hop *ip-address* [**...***ip-address*]

Syntax Description

ip-address	IP address of the next hop to which packets are output. It must be the address of an adjacent router.
dynamic dhcp	Sets dynamically the DHCP next hop.
encapsulate l3vpn	Sets the encapsulation profile for VPN nexthop.
profile name	The L3VPN encapsulation profile name.
peer-address	Sets the next hop to be the BGP peering address.
recursive *ip-address*	Sets the IP address of the recursive next-hop router. **Note** The next-hop IP address must be assigned separately from the recursive next-hop IP address.
global	Sets the global routing table.
vrf *vrf name*	Sets the VRF.
verify- availability	Verifies if the nexthop is reachable.
sequence	(Optional) The sequence to insert into next-hop list. The range is from 1 to 65535.
track	(Optional) Sets the next hop depending on the state of a tracked object.
track object number	(Optional) The tracked object number. The range is from 1 to 500.

Command Default

Packets are forwarded to the next hop router in the routing table.

Command Modes

Route-map configuration (config-route-map)

Command History	Release	Modification
	11.0	This command was introduced.
	12.0(28)S	The **recursive** keyword was added.
	12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
	Cisco IOS XE Release 2.2	In Cisco IOS XE Release 2.2 this command was introduced on the Cisco ASR 1000 Series Routers.
	12.2(33)SRE	This command was modified. The **encapsulatel3vpn** keyword was added.

Usage Guidelines

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *ip-address* argument .

Use the **ippolicyroute-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 **ippolicyroute-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 *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.

If the interface associated with the first next hop specified with the **setipnext-hop**command is down, the optionally specified IP addresses are tried in turn.

The set clauses can be used in conjunction with one another. They are evaluated in the following order:

1 **set ip next-hop**
2 **set interface**
3 **set ip default next-hop**
4 **set default interface**

Note   The set ip next-hop and set ip default next-hop are similar commands but have a different order of operations. Configuring the set ip next-hop command causes the system to use policy routing first and then use the routing table. Configuring the set ip default next-hop command causes the system to use the routing table first and then policy route the specified next hop.

Command Examples In the following example, packets with a Level 3 length of 3 to 50 bytes are output to the router at IP address 10.14.2.2:

```
interface serial 0
 ip policy route-map thataway
!
route-map thataway
 match length 3 50
 set ip next-hop 10.14.2.2
```

In the following example, the IP address of 10.3.3.3 is set as the recursive next-hop address:

```
route-map map_recurse
 set ip next-hop recursive 10.3.3.3
```

Related Commands

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

set ip next-hop verify-availability

To configure policy routing to verify the reachability of the next hop of a route map before the router performs policy routing to that next hop, use the **setipnext-hopverify-availability**command in route-map configuration mode. To disable this function, use the **no** form of this command.

> **set ip next-hop verify-availability** [*next-hop-address sequence* **track** *object*]

> **no set ip next-hop verify-availability** [*next-hop-address sequence* **track** *object*]

Syntax Description

next-hop-address	(Optional) IP address of the next hop to which packets will be forwarded.
sequence	(Optional) Sequence of next hops. The acceptable range is from 1 to 65535.
track	(Optional) The tracking method is track.
object	(Optional) Object number that the tracking subsystem is tracking. The acceptable range is from 1 to 500.

Command Default

The reachability of the next hop of a route map before a router performs policy routing, is not verified.

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.3(4)T	The optional **track** keyword and *next-hop-address*, *sequence*, and *object* arguments were added.
12.3(14)T	The SAA feature (uses **rtr** commands) was replaced by the IP SLAs feature (uses **ipsla** commands).
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.2	In Cisco IOS XE Release 2.2 this command was introduced on the Cisco ASR 1000 Series Routers.

Usage Guidelines   The **setipnext-hopverify-availability** command can be used in the following two ways:

- With policy-based routing (PBR) to verify next hop reachability using Cisco Discovery Protocol (CDP).
- With optional arguments to support object tracking using Internet Control Message Protocol (ICMP) ping or an HTTP GET request to verify if a remote device is reachable.

Using CDP Verification

This command is used to verify that the next hop is reachable before the router tries to policy route to it. This command has the following characteristics:

- It causes some performance degradation.
- CDP must be configured on the interface.
- The next hop must be a Cisco device with CDP enabled.
- It is supported in process switching and Cisco Express Forwarding (CEF) policy routing, but is not available in distributed CEF (dCEF) because of the dependency of the CDP neighbor database.

If the router is policy routing packets to the next hop and the next hop is down, the router will try unsuccessfully to use Address Resolution Protocol (ARP) for the next hop (which is down). This behavior will continue indefinitely. To prevent this situation from occurring, use the **setipnext-hopverify-availability** command to configure the router to verify that the next hop of the route map is a CDP neighbor before routing to that next hop.

This command is optional because some media or encapsulations do not support CDP, or it may not be a Cisco device that is sending traffic to the router.

If this command is set and the next hop is not a CDP neighbor, then the router looks to the subsequent next hop, if there is one. If there is no next hop, the packets are not policy routed.

If this command is not set, the packets are either successfully policy routed or remain forever unrouted.

If you want to selectively verify availability of only some next hops, you can configure different route map entries (under the same route map name) with different criteria (using access list matching or packet size matching), and then use the**setipnext-hopverify-availability** command selectively.

Using Object Tracking

With optional arguments to support object tracking, this command allows PBR to make decisions based on the following criteria:

- ICMP ping reachability to a remote device.
- Application running on a remote device (for example, the device responds to an HTTP GET request).
- A route exists in the Routing Information Base (RIB) (for example, policy route only if 10.2.2.0/24 is in the RIB).

- Interface state (for example, packets received on E0 should be policy routed out E1 only if E2 is down).

Object tracking functions in the following manner. PBR will inform the tracking process that it is interested in tracking a certain object. The tracking process will in turn notify PBR when the state of the object changes. This notification is done via registries and is event driven.

The tracking subsystem is responsible for tracking the state of an object. The object can be an IP address that is periodically being pinged by the tracking process. The state of the object (up or down) is stored in a track report data structure. The tracking process will create the tracking object report. Then the exec process that is configuring the route map can query the tracking process to determine if a given object exists. If the object exists, the tracking subsystem can start tracking it and read the initial state of the object. If the object changes state, the tracking process will notify all the clients that are tracking this process that the state of the object has changed. So, the route map structure that PBR is using can be updated to reflect the current state of the object in the track report. This interprocess communication is done by means of registries and the shared track report.

> **Note** If the CDP and object tracking commands are mixed, the tracked next hops will be tried first.

Command Examples
The following configuration sample demonstrates the use of the **setnext-hopverify-availability** command to configure the router to verify that the next hop of the route map is a CDP neighbor before routing to that next hop. In this example, the next hop 10.0.0.8 in the route map named "Example1" will be verified as a CDP neighbor before the router tries to policy-route to it.

```
ip cef
interface ethernet0/0/1
 ip policy route-map Example1
 exit
route-map Example1 permit 10
 match ip address 1
 set ip precedence priority
 set ip next-hop 10.0.0.8
 set ip next-hop verify-availability
 exit
route-map Example1 permit 20
 match ip address 101
 set interface Ethernet0/0/3
 set ip tos max-throughput
 end
```

Examples
The following configuration sample shows a configuration used to track an object:

```
! Configure the objects to be tracked.
! Object 123 will be up if the router can ping 10.1.1.1.
! Object 124 will be up if the router can ping 10.2.2.2.
ip sla monitor 1
 type echo protocol ipicmpecho 10.1.1.1
ip sla monitor schedule 1 start-time now life forever
!
ip sla monitor 2
 type echo protocol ipicmpecho 10.2.2.2
ip sla monitor schedule 2 start-time now life forever
!
track 123 rtr 1 reachability
track 124 rtr 2 reachability
```

```
!
! Enable policy routing using route-map alpha on Ethernet 0.
interface ethernet 0
 ip address 10.4.4.254 255.255.255.0
 ip policy route-map alpha
!
! 10.1.1.1 is via this interface
interface ethernet 1
 ip address 10.1.1.254 255.255.255.0
! 10.2.2.2 is via this interface
interface ethernet 2
 ip address 10.2.2.254 255.255.255.0
!
! Configure a route-map to set the next-hop to 10.1.1.1 if object 123 is up. If object 123
! is down, the next hop will be set to 10.2.2.2 if object 124 is up. If object 124 is also
! down, then policy routing fails and unicast routing will route the packet.
route-map alpha
 set ip next-hop verify-availability 10.1.1.1 10 track 123
 set ip next-hop verify-availability 10.2.2.2 20 track 124
```

Related Commands

Command	Description
show route-map	Displays the configured route maps.
show track	Displays information about objects that are tracked by the tracking process.
track	Tracks the state of an interface, an ip route, or a response time reporter.

set ip vrf

To indicate where to forward packets that pass a match clause of a route map for policy routing when the next hop must be under a specified virtual routing and forwarding (VRF) name, use the **setipvrf**command in route-map configuration mode. To disable this feature, use the **no** form of this command.

> **set ip vrf** *vrf-name* **next-hop** {*ip-address* [... *ip-address*] | **recursive** *ip-address*}

> **no set ip vrf** *vrf-name* **next-hop** {*ip-address* [... *ip-address*] | **recursive** *ip-address*}

Syntax Description

vrf-name	Name of the VRF.
next - **hop** *ip-address*	IP address of the next hop to which packets are forwarded. The next hop must be an adjacent router.
next - **hop recursive** *ip-address*	IP address of the recursive next-hop router. **Note** The next-hop IP address must be assigned separately from the recursive next-hop IP address.

Command Default

Policy-based routing is not applied to a VRF interface.

Command Modes

Route-map configuration

Command History

Release	Modification
12.2(33)SXH5	This command was introduced.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.

Usage Guidelines

The **setipvrf**command allows you to apply policy-based routing to a VRF interface.

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *ip-address* argument.

Use the **ippolicyroute-map** interface configuration command, the **route-map**global configuration command, and **match**configuration commands to define the conditions for policy-routing packets. The **ippolicyroute-map** command identifies a route map by name. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the match criteria--the

conditions under which policy routing occurs. The **set**commands specify the set actions--the particular routing actions to perform if the criteria enforced by the **match** commands are met.

If the interface associated with the first next hop specified with the **setipvrf**command is down, the optionally specified IP addresses are tried in turn.

The set clauses can be used in conjunction with one another. They are evaluated in the following order:

1 set TOS
2 set DF (Don't Fragment) bit in IP header
3 set vrf
4 set ip next-hop
5 set interface
6 set ip default next-hop
7 set default interface

Command Examples

The following example specifies that the next hop must be under the VRF name that has the IP address 10.5.5.5:

```
set ip vrf myvrf next-hop 10.5.5.5
```

Related Commands

Command	Description
ip policy route-map	Identifies a route map to use for policy routing on an interface.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match length	Bases policy routing on the Level 3 length of a packet.
route-map	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 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 Cisc 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 level (IP)

To indicate where to import routes, use the **setlevel** command in route-map configuration mode. To delete an entry, use the **no** form of this command.

set level {**level-1** | **level-2** | **level-1-2** | **nssa-only** | **stub-area** | **backbone**}

no set level {**level-1** | **level-2** | **level-1-2** | **nssa-only** | **stub-area** | **backbone**}

Syntax Description

level-1	Imports routes into a Level 1 area.
level-2	Imports routes into a Level 2 subdomain.
level-1-2	Imports routes into Level 1 and Level 2 areas.
nssa-only	Imports routes only into NSSA areas.
stub-area	Imports routes into an Open Shortest Path First (OSPF) NSSA area.
backbone	Imports routes into an OSPF backbone area.

Command Default

This command is disabled by default. For Intermediate System-to-Intermediate System (IS-IS) destinations, the default value is **level-2**.

Command Modes

Route-map configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	This command was modified. The nssa-only keyword was added.

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 **set** route-map configuration commands specify the redistribution *setactions* to be performed when all the match criteria of a route map are met. When all match criteria are met, all set actions are performed.

The **stub-areaandbackbonekeywordshavenoeffectonwhereroutesareimported.**

Command Examples

In the following example, routes will be imported into the Level 1 area:

```
route-map name
 set level level-1
```

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 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 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 automatic-tag	Automatically computes the tag value.

Command	Description
set community	Sets the BGP communities attribute.
set ip next-hop	Specifies the address of the next hop.
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 origin (BGP)	Sets the BGP origin code.
set tag (IP)	Sets the value of the destination routing protocol.

set local-preference

To specify a preference value for the autonomous system path, use the**setlocal-preference** command in route-map configuration mode. To delete an entry, use the**no**form of this command.

set local-preference commandset local-preference *number-value*

no set local-preference *number-value*

Syntax Description

number-value	Preference value. An integer from 0 to 4294967295.

Command Default

Preference value of 100

Command Modes

Route-map configuration

Command History

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

Usage Guidelines

The preference is sent only to all routers in the local autonomous system.

You must have a match clause (even if it points to a "permit everything" list) if you want to set tags.

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 **set** route-map configuration commands specify the redistribution *setactions* to be performed when all the match criteria of a route map are met. When all match criteria are met, all set actions are performed.

You can change the default preference value with thebgp default local-preferencecommand.

Command Examples   The following example sets the local preference to 100 for all routes that are included in access list 1:

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

Related Commands

Command	Description
bgp default local-preference	Changes the default local preference value.
match as-path	Matches a BGP autonomous system path access list.
match community	Matches a BGP community.
match interface (IP)	Distributes 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 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 automatic-tag	Automatically computes the tag value.
set community	Sets the BGP communities attribute.
set ip next-hop	Specifies the address of the next hop.
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.

Command	Description
set metric-type	Sets the metric type for the destination routing protocol.
set origin (BGP)	Sets the BGP origin code.
set tag (IP)	Sets the value of the destination routing protocol.

set metric (BGP-OSPF-RIP)

To set the metric value for a routing protocol, use the **setmetric** command in route-map configuration mode. To return to the default metric value, use the **no** form of this command.

> **set metric** *metric-value*
>
> **no set metric** *metric-value*

Syntax Description

metric-value	Metric value; an integer from -294967295 to 294967295. This argument applies to all routing protocols except Enhanced Interior Gateway Routing Protocol (EIGRP).

Command Default

The dynamically learned metric value.

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.

Usage Guidelines

We recommend that you consult your Cisco technical support representative before changing the default value.

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 **set** route-map configuration commands specify the redistribution *setactions* to be performed when all the match criteria of a route map are met. When all match criteria are met, all set actions are performed.

Command Examples   The following example sets the metric value for the routing protocol to 100:

```
route-map set-metric
 set metric 100
```

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 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 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 automatic-tag	Automatically computes the tag value.
set community	Sets the BGP communities attribute.
set ip next-hop	Specifies the address of the next hop.
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.

Command	Description
set origin (BGP)	Sets the BGP origin code.
set tag (IP)	Sets the value of the destination routing protocol.

set metric-type

To set the metric type for the destination routing protocol, use the **setmetric-type** command in route-map configuration mode. To return to the default, use the **no** form of this command.

set metric-type commandset metric-type {**internal** | **external** | **type-1** | **type-2**}

no set metric-type {**internal** | **external** | **type-1** | **type-2**}

Syntax Description

internal	Intermediate System-to-Intermediate System (IS-IS) internal metric, or IGP metric as the MED for BGP.
external	IS-IS external metric.
type-1	Open Shortest Path First (OSPF) external Type 1 metric.
type-2	OSPF external Type 2 metric.

Command Default

This command is disabled by default.

Command Modes

Route-map configuration

Command History

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

Usage Guidelines

Use the **route-map** global configuration command with **match** and **set** route-map configuration commands to define the conditions for redistributing routes from one routing protocol into another. 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 **set** route-map configuration commands specify the redistribution *setactions* to be performed when all the match criteria of a route map are met. When all match criteria are met, all set actions are performed.

Note   This command is not supported for redistributing routes into Border Gateway Protocol (BGP).

Command Examples   The following example sets the metric type of the destination protocol to OSPF external Type 1:

```
route-map map-type
 set metric-type type-1
```

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 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 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 automatic-tag	Automatically computes the tag value.
set community	Sets the BGP communities attribute.
set ip next-hop	Specifies the address of the next hop.

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 origin (BGP)	Sets the BGP origin code.
set tag (IP)	Sets the value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.

set next-hop

To specify the address of the next hop, use the**setnext-hop** command in route-map configuration mode. To delete an entry, use the **no** form of this command.

set next-hop commandset next-hop *next-hop*

no set next-hop *next-hop*

Syntax Description

next-hop	IP address of the next hop router.

Command Default

Default next hop address.

Command Modes

Route-map configuration

Command History

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

Usage Guidelines

You must have a match clause (even if it points to a "permit everything" list) if you want to set tags.

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 **set** route-map configuration commands specify the redistribution *setactions* to be performed when all the match criteria of the router are met. When all match criteria are met, all set actions are performed.

Command Examples In the following example, routes that pass the access list have the next hop set to 172.160.70.24:

```
route-map map_hop
 match address 5
 set next-hop 172.160.70.24
```

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 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 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 automatic-tag	Automatically computes the tag value.
set community	Sets the BGP communities attribute.
set ip next-hop	Specifies the address of the next hop.
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.

Command	Description
set metric-type	Sets the metric type for the destination routing protocol.
set origin (BGP)	Sets the BGP origin code.
set tag (IP)	Sets the value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.

set tag (IP)

To set a tag value of the destination routing protocol, use the **settag** command in route-map configuration mode. To delete the entry, use the **no** form of this command.

> **set tag commandset tag** *tag-value*
>
> **no set tag** *tag-value*

Syntax Description

tag-value	Name for the tag. Integer from 0 to 4294967295.

Command Default

If not specified, the default action is to *forward* the tag in the source routing protocol onto the new destination protocol.

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.

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 **set** route-map configuration commands specify the redistribution *setactions* to be performed when all the match criteria of a route map are met. When all match criteria are met, all set actions are performed.

Command Examples   The following example sets the tag value of the destination routing protocol to 5:

```
Router(config)# route-map tag
Router(config-router)#  set tag 5
```

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 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 route-type (IP)	Redistributes routes of the specified type.
match tag	Redistributes routes in the routing table that match the specified tags.
route-map	Defines the conditions for redistributing routes from one routing protocol into another.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set automatic-tag	Automatically computes the tag value.
set community	Sets the BGP communities attribute.
set ip next-hop	Specifies the address of the next hop.
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.

Command	Description
set metric-type	Sets the metric type for the destination routing protocol.
set origin (BGP)	Sets the BGP origin code.
set tag (IP)	Sets the value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.

show bfd drops

To display the number of dropped packets in Bidirectional Forwarding Detection (BFD), use the **showbfddrops**command in user EXEC or privileged EXEC mode.

show bfd drops

Syntax Description   This command has no arguments or keywords.

Command Modes   User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
15.1(2)S	This command was introduced.
15.1(3)S	This command was modified. The output was enhanced to display authentication information for multihop sessions.

Command Examples   The following sample output from the **showbfddrops** command shows a multihop session with authentication enabled. The IPV4-M and IPV6-M columns display multihop session counters for IPv4 and IPv6, respectively.

```
Router# show bfd drops

BFD Drop Statistics
                      IPV4    IPV6    IPV4-M  IPV6-M  MPLS_PW MPLS_TP_LSP
Invalid TTL           0       0       0       0       0       0
BFD Not Configured    0       0       0       0       0       0
No BFD Adjacency      0       0       0       0       0       0
Invalid Header Bits   0       0       0       0       0       0
Invalid Discriminator 0       0       0       0       0       0
Session AdminDown     0       0       0       0       0       0
Authen invalid BFD ver 0      0       0       0       0       0
Authen invalid len    0       0       0       0       0       0
Authen invalid seq    0       0       0       0       0       0
Authen failed         0       0       0       0       0       0
```

The table below describes the significant fields shown in the displays.

Table 2   *show bfd drops* **Field Descriptions**

Field	Description
Invalid Header Bits	Some header bits are invalid or unexpected.

Field	Description
BFD Not Configured	A packet was received for a session that does not exist.
Invalid Discriminator	Invalid or unexpected discriminator ID.
Authen invalid BFD ver	An authenticated packet was received in a BFD session with a version that does not support authentication.
Authen invalid len	An authenticated packet was received with an invalid authentication length.
Authen invalid seq	An authenticated packet was received with an invalid authentication sequence.

Related Commands

Command	Description
show bfd neighbors	Displays a line-by-line listing of existing BFD adjacencies
show bfd summary	Displays summary information for BFD.

show bfd neighbors

To display a line-by-line listing of existing Bidirectional Forwarding Detection (BFD) adjacencies, use the **showbfdneighbors**command in user EXEC or privileged EXEC mode.

> **show bfd neighbors** [**client** {**bgp** | **eigrp** | **isis** | **ospf** | **rsvp** | **te-frr**} | **details** | [*interface-type interface-number*] | **internal** | **ipv4** *ip-address* | **ipv6** *ipv6-address* | **vrf** *vrf-name*]

Syntax Description

client	(Optional) Displays the neighbors of a specific client.
bgp	(Optional) Specifies a Border Gateway Protocol (BGP) client.
eigrp	(Optional) Specifies an Enhanced Interior Gateway Routing Protocol (EIGRP) client.
isis	(Optional) Specifies an Intermediate System-to-Intermediate System (IS-IS) client.
ospf	(Optional) Specifies an Open Shortest Path First (OSPF) client.
rsvp	(Optional) Specifies a Resource Reservation Protocol (RSVP) client.
te-frr	(Optional) Specifies a traffic engineering (TE) Fast Reroute (FRR) client.
details	(Optional) Displays all BFD protocol parameters and timers for each neighbor.
interface-type interface-number	(Optional) Neighbors at a specified interface.
internal	(Optional) Displays internal BFD information.
ipv4	(Optional) Specifies an IPv4 neighbor. If the **ipv4** keyword is used without the *ip-address* argument, all IPv4 sessions are displayed.
ip-address	(Optional) IP address of a neighbor in A.B.C.D format.
ipv6	(Optional) Specifies an IPv6 neighbor. If the **ipv6** keyword is used without the *ipv6-address* argument, all IPv6 sessions are displayed.
ipv6-address	(Optional) IPv6 address of a neighbor in X:X:X:X::X format.

vrf *vrf-name*	(Optional) Displays entries for a specific VPN routing and forwarding (VRF) instance.

Command Modes   User EXEC (>) Privileged EXEC (#)

Command History

S Release	Modification
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S.
12.2(18)SXE	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRC	This command was modified. The **vrf***vrf-name* keyword and argument, the **client** keyword, and the *ip-address*argument were added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was modified. The output was modified to display the "OurAddr" field only with the **details** keyword.
12.2(33)SRE	This command was modified. Support for IPv6 was added.
15.1(2)S	This command was modified. • The **showbfdneighborsdetails** command output was changed for hardware-offloaded BFD sessions. • The**showbfdneighbors**command output was changed to show the header type identifying the session type.
15.1(3)S	This command was modified to display information for multihop sessions.
T Release	Modification
12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.
12.4(9)T	This command was modified. Support for BFD Version 1 and BFD echo mode was added.

S Release	Modification
15.1(2)T	This command was modified. Support for IPv6 was added.

X Release	Modification
Cisco IOS XE Release 2.1	This command was modified. Support for IPv6 was added.

Usage Guidelines

The **showbfdneighbors** command can be used to help troubleshoot the BFD feature.

The full output for the **details** keyword is not supported on the Route Processor (RP) for the Cisco 12000 series Internet router. If you want to enter the **showbfdneighbors** 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 **showbfdneighborsdetails** command will show the configured intervals, not the changed ones.

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

Command Examples

Examples

The following sample output shows the status of the adjacency or neighbor:

```
Router# show bfd neighbors
OurAddr        NeighAddr      LD/RD RH  Holdown(mult) State     Int
172.16.10.1    172.16.10.2    1/6   1   260 (3 )      Up        Fa0/1
```

The following sample output from the **showbfdneighbors** command entered with the **details** keyword shows BFD protocol parameters and timers for each neighbor:

```
Router# show bfd neighbors details
NeighAddr                           LD/RD    RH/RS     State     Int
10.1.1.2                            1/1       1(RH) Up         Et0/0
Session state is UP and not using echo function.
OurAddr: 10.1.1.1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 50000, Multiplier: 3 Received MinRxInt: 50000, Received
Multiplier: 3 Holddown (hits): 150(0), Hello (hits): 50(2223) Rx Count: 2212, Rx Interval
(ms) min/max/avg: 8/68/49 last: 0 ms ago Tx Count: 2222, Tx Interval (ms) min/max/avg:
40/60/49 last: 20 ms ago Elapsed time watermarks: 0 0 (last: 0) Registered protocols: CEF
Stub
Uptime: 00:01:49
Last packet: Version: 0               - Diagnostic: 0
            I Hear You bit: 1          - Demand bit: 0
            Poll bit: 0                - Final bit: 0
            Multiplier: 3              - Length: 24
            My Discr.: 1               - Your Discr.: 1
            Min tx interval: 50000     - Min rx interval: 50000
            Min Echo interval: 50000
```

The following sample output from the RP on a Cisco 12000 series Internet router shows the status of the adjacency or neighbor:

```
Router# show bfd neighbors
Cleanup timer hits: 0
OurAddr       NeighAddr      LD/RD RH  Holdown(mult)  State     Int
172.16.10.2   172.16.10.1    2/0   0   0    (0 )      Up        Fa6/0
 Total Adjs Found: 1
```

The following sample output from the RP on a Cisco 12000 series Internet router shows the status of the adjacency or neighbor with the **details** keyword:

```
Router# show bfd neighbors details
Cleanup timer hits: 0
OurAddr       NeighAddr      LD/RD RH  Holdown(mult)  State     Int
172.16.10.2   172.16.10.1    2/0   0   0    (0 )      Up        Fa6/0
Registered protocols: OSPF
Uptime: never
%% BFD Neighbor statistics are not available on RP. Please execute this command on Line
Card.
```

The following sample output from a line card on a Cisco 12000 series Internet router shows the status of the adjacency or neighbor:

```
Router# attach 6
Entering Console for 8 Port Fast Ethernet in Slot: 6
Type "exit" to end this session
Press RETURN to get started!
Router> show bfd neighbors
Cleanup timer hits: 0
OurAddr       NeighAddr      LD/RD RH  Holdown(mult)  State     Int
172.16.10.2   172.16.10.1    2/1   1   848  (5 )      Up        Fa6/0
 Total Adjs Found: 1
```

The following sample output from a line card on a Cisco 12000 series Internet router shows the status of the adjacency or neighbor with the **details** keyword:

```
Router# attach 6
Entering Console for 8 Port Fast Ethernet in Slot: 6
Type "exit" to end this session
Press RETURN to get started!
Router>
show bfd neighbors details
Cleanup timer hits: 0
OurAddr       NeighAddr      LD/RD RH  Holdown(mult)  State     Int
172.16.10.2   172.16.10.1    2/1   1   892  (5 )      Up        Fa6/0
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 1000, Multiplier: 3
Received MinRxInt: 200000, Received Multiplier: 5
Holdown (hits): 1000(0), Hello (hits): 200(193745)
Rx Count: 327406, Rx Interval (ms) min/max/avg: 152/248/196 last: 108 ms ago
Tx Count: 193748, Tx Interval (ms) min/max/avg: 204/440/331 last: 408 ms ago
Last packet: Version: 0         - Diagnostic: 0
             I Hear You bit: 1   - Demand bit: 0
             Poll bit: 0         - Final bit: 0
             Multiplier: 5       - Length: 24
             My Discr.: 1        - Your Discr.: 2
             Min tx interval: 200000    - Min rx interval: 200000
             Min Echo interval: 0
Uptime: 17:54:07
SSO Cleanup Timer called: 0
SSO Cleanup Action Taken: 0
Pseudo pre-emptive process count: 7728507 min/max/avg: 8/16/8 last: 12 ms ago
 IPC Tx Failure Count: 0
 IPC Rx Failure Count: 0
 Total Adjs Found: 1
LC-Slot6>
```

Examples

The following sample output verifies that the BFD neighbor router is also running BFD Version 1 and that the BFD session is up and running in echo mode:

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

Examples

The following example displays all IPv6 sessions:

```
Router# s
how bfd neighbors ipv6 2001::1
OurAddr    NeighAddr  LD/RD  RH/RS  Holddown(mult)  State  Int
1:1::5     1:1::6     2/2    Up     0    (3 )   Up     Et0/0
2:2::5     2:2::6     4/4    Up     0    (3 )   Up     Et1/0
```

Examples

The following is sample output from the **show bfd neighbors** command:

```
Router# show bfd neighbors
NeighAddr                          LD/RD    RH/RS     State     Int
192.0.2.1                          4/0      Down      Down      Et0/0
192.0.2.2                          5/0      Down      Down      Et0/0
192.0.2.3                          6/0      Down      Down      Et0/0
192.0.2.4                          7/0      Down      Down      Et0/0
192.0.2.5                          8/0      Down      Down      Et0/0
192.0.2.6                          11/0       0(RH) Fail       Et0/0
1000:1:1:1:1:1:1:2                 9/0      Down      Down      Et0/0
1000:1:1:1:1:1:1:810               10/0     Down      Down      Et0/0
1000:1111:1111:111:11:111:11:5     1/0        0(RH) Fail       Et0/0
1000:1111:1111:111:11:111:11:6     2/0      Down      Down      Et0/0
1000:1111:1111:1111:1111:1111:1111:8810
                                   3/0      Down      Down      Et0/0
```

The following is sample output from the **show bfd neighbors details** command:

```
Router# show bfd neighbors details
NeighAddr                          LD/RD    RH/RS     State     Int
192.0.2.5                          4/0      Down      Down      Et0/0
OurAddr: 192.0.2.8
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3
Received MinRxInt: 0, Received Multiplier: 0
Holddown (hits): 0(0), Hello (hits): 1000(120)
Rx Count: 0, Rx Interval (ms) min/max/avg: 0/0/0 last: 118672 ms ago
Tx Count: 120, Tx Interval (ms) min/max/avg: 760/1000/885 last: 904 ms ago
Elapsed time watermarks: 0 0 (last: 0)
Registered protocols: Stub
Last packet: Version: 1          - Diagnostic: 0
```

```
               State bit: AdminDown  - Demand bit: 0
               Poll bit: 0           - Final bit: 0
               Multiplier: 0         - Length: 0
               My Discr.: 0          - Your Discr.: 0
               Min tx interval: 0    - Min rx interval: 0
               Min Echo interval: 0

NeighAddr                          LD/RD    RH/RS     State     Int
1000:1:1:1:1:1:1:2                 9/0      Down      Down      Et0/0
OurAddr: 1000:1:1:1:1:1:1:1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3
Received MinRxInt: 0, Received Multiplier: 0
Holddown (hits): 0(0), Hello (hits): 1000(208)
Rx Count: 0, Rx Interval (ms) min/max/avg: 0/0/0 last: 194760 ms ago
Tx Count: 208, Tx Interval (ms) min/max/avg: 760/1000/878 last: 424 ms ago
Elapsed time watermarks: 0 0 (last: 0)
Registered protocols: Stub
Last packet: Version: 1           - Diagnostic: 0
               State bit: AdminDown  - Demand bit: 0
               Poll bit: 0           - Final bit: 0
               Multiplier: 0         - Length: 0
               My Discr.: 0          - Your Discr.: 0
               Min tx interval: 0    - Min rx interval: 0
               Min Echo interval: 0
```

The table below describes the significant fields shown in the displays.

Table 3   *show bfd neighbors* **Field Descriptions**

Field	Description
OurAddr	IP address of the interface for which the **showbfdneighborsdetails**command was entered.
NeighAddr	IPv4 or IPv6 address of the BFD adjacency or neighbor.
LD/RD	Local discriminator and remote discriminator being used for the session.
RH	Remote Heard--Indicates that the remote BFD neighbor has been heard.
Holddown(mult)	The detect timer multiplier that is used for this session.
State	State of the interface--Up or Down.
Int	Interface type and slot/port.
Session state is UP and using echo function with 50 ms interval.	BFD is up and running in echo mode. The 50-millisecond interval has been adopted from the **bfd** command. **Note** BFD Version 1 and echo mode are supported only with Cisco IOS Release 12.4(9)T and later releases.
Rx Count	Number of BFD control packets that have been received from the BFD neighbor.

Field	Description
Tx Count	Number of BFD control packets that have been sent by the BFD neighbor.
Tx Interval	The interval, in milliseconds, between sent BFD packets.
Registered protocols	Routing protocols that have been registered with BFD.
Last packet: Version:	BFD version detected and run between the BFD neighbors. The system automatically performs BFD version detection, and BFD sessions between neighbors will run in the highest common BFD version between neighbors. For example, if one BFD neighbor is running BFD Version 0, and the other BFD neighbor is running Version 1, the session will run BFD Version 0. **Note** BFD Version 1 and echo mode are supported only with Cisco IOS Release 12.4(9)T and later releases.
Diagnostic	A diagnostic code specifying the local system's reason for the last transition of the session from Up to some other state. State values are as follows: • 0--No Diagnostic • 1--Control Detection Time Expired • 2--Echo Function Failed • 3--Neighbor Signaled Session Down • 4--Forwarding Plane Reset • 5--Path Down • 6--Concentrated Path Down • 7--Administratively Down
I Hear You bit	The I Hear You Bit is set to 0 if the transmitting system is either not receiving BFD packets from the remote system or is tearing down the BFD session for some reason. During normal operation, the I Hear You bit is set to 1 to signify that the remote system is receiving the BFD packets from the transmitting system.
Demand bit	Demand Mode bit. BFD has two modes-- asynchronous and demand. If the Demand Mode is set, the transmitting system prefers to operate in demand mode. The Cisco implementation of BFD supports only asynchronous mode.

Field	Description
Poll bit	If the Poll bit is set, the transmitting system is requesting verification of connectivity or verification of a parameter change.
Final bit	If the Final bit is set, the transmitting system is responding to a received BFD control packet that had a Poll (P) bit set.
Multiplier	Detect time multiplier. The negotiated transmit interval multiplied by the detect time multiplier determines the detection time for the transmitting system in BFD asynchronous mode.
	The detect time multiplier is similar to the hello multiplier in Intermediate System-to-Intermediate System (IS-IS), which is used to determine the hold timer: (hello interval) * (hello multiplier) = hold timer. If a hello packet is not received within the hold-timer interval, a failure has occurred.
	Similarly, for BFD: (transmit interval) * (detect multiplier) = detect timer. If a BFD control packet is not received from the remote system within the detect-timer interval, a failure has occurred.
Length	Length of the BFD control packet, in bytes.
My Discr.	My Discriminator. Unique, nonzero discriminator value generated by the transmitting system used to demultiplex multiple BFD sessions between the same pair of systems.
Your Discr.	Your Discriminator. The discriminator received from the corresponding remote system. This field reflects the received value of My Discriminator, or is zero if that value is unknown.
Min tx interval	Minimum transmission interval, in microseconds, that the local system wants to use when sending BFD control packets.
Min rx interval	Minimum receipt interval, in microseconds, between received BFD control packets that the system can support.

Field	Description
Min Echo interval	Minimum interval, in microseconds, between received BFD control packets that the system can support. If the value is zero, the transmitting system does not support the receipt of BFD echo packets.
	The Cisco implementation of BFD for Cisco IOS Releases 12.2(18)SXE and 12.0(31)S does not support the use of echo packets.

Examples

The following is sample output from the **show bfd neighbors details** command for BFD sessions offloaded to hardware. The Rx and Tx counts show the number of packets received and transmitted by the BFD session in hardware.

```
NeighAddr                               LD/RD        RH/RS      State      Int
192.0.2.1                               298/298      Up         Up         Te7/1.2
Session state is UP and not using echo function.
Session Host: Hardware - session negotiated with platform adjusted timer values.
              Holddown - negotiated: 510000      adjusted: 0
OurAddr: 192.0.2.2
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 170000, MinRxInt: 170000, Multiplier: 3
Received MinRxInt: 160000, Received Multiplier: 3
Holddown (hits): 0(0), Hello (hits): 170(0)
Rx Count: 1256983
Tx Count: 24990
Elapsed time watermarks: 0 0 (last: 0)
Registered protocols: OSPF CEF
Uptime: 18:11:31
Last packet: Version: 1                - Diagnostic: 0
             State bit: Up             - Demand bit: 0
             Poll bit: 0               - Final bit: 0
             Multiplier: 3             - Length: 24
             My Discr.: 298             - Your Discr.: 298
             Min tx interval: 160000   - Min rx interval: 160000
             Min Echo interval: 0
```

Examples

The following is sample output from the **show bfd neighbors** command showing a header type identifying the type of session:

```
Router# show bfd neighbors

MPLS-TP Sessions
Interface       LSP type                LD/RD      RH/RS      State
Tunnel-tp1      Working                 1/0        Down       Down
Tunnel-tp2      Working                 3/0        Down       Down
Tunnel-tp1      Protect                 2/0        Down       Down


IPv4 Sessions
NeighAddr                       LD/RD      RH/RS      State      Int
192.0.2.1                       2/0        Down       Down       Et2/0
```

The following is sample output from the **show bfd neighbors** command for Virtual Circuit Connection Verification (VCCV) sessions:

```
Router# show bfd neighbors
VCCV Sessions
```

```
Peer Addr      :VCID                        LD/RD   RH/RS     State
198.51.100.1   :100                         1/1     Up        Up
```

The following is sample output from the **show bfd neighbors** command for IPv4 and IPv6 sessions:

```
Router# show bfd neighbors

IPv4 Sessions
NeighAddr                        LD/RD   RH/RS     State     Int
192.0.2.1                        6/0     Down      Down      Et1/0
203.0.113.1                      7/6     Up        Up        Et3/0
198.51.100.2                     8/7     Up        Up        Et0/0
IPv6 Sessions
NeighAddr                        LD/RD   RH/RS     State     Int
CC::2                            1/1     Up        Up        Et0/0
DD::2                            2/2     Up        Up        Et0/0
EE::2                            3/3     Up        Up        Et0/0
ABCD::2                          4/4     Up        Up        Et0/0
FE80::2                          5/5     Up        Up        Et0/0
```

The table below describes the significant fields shown in the displays.

Table 4   show bfd neighbors Field Descriptions

Field	Description
Interface	Name of the MPLS tunnel TP interface.
LSP type	Type of label switched path for this session (Working or Protect).

Examples

The following is sample output from the show bfd neighbors command for a single-hop session:

```
Router# show bfd neighbors

IPv4 Sessions
NeighAddr                            LD/RD       RH/RS     State     Int
192.0.0.2                            1/12        Up        Up        Et0/0
Session state is UP and using echo function with 300 ms interval.
Session Host: Software
OurAddr: 192.0.0.1
Handle: 12
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3
Received MinRxInt: 1000000, Received Multiplier: 3
Holddown (hits): 0(0), Hello (hits): 1000(62244)
Rx Count: 62284, Rx Interval (ms) min/max/avg: 1/2436/878 last: 239 ms ago
Tx Count: 62247, Tx Interval (ms) min/max/avg: 1/1545/880 last: 246 ms ago
Elapsed time watermarks: 0 0 (last: 0)
Registered protocols: Stub CEF
Uptime: 00:22:06
Last packet: Version: 1                 - Diagnostic: 0
             State bit: Up              - Demand bit: 0
             Poll bit: 0                - Final bit: 0
             Multiplier: 3              - Length: 24
             My Discr.: 12              - Your Discr.: 1
             Min tx interval: 1000000   - Min rx interval: 1000000
             Min Echo interval: 300000
```

Examples

The following is sample output from the show bfd neighbors command for an IPv4 multihop session. The section headed "Map information:" has information specific to the multihop session.

```
Router# show bfd neighbors

IPv4 Multihop Sessions
NeighAddr[vrf]                                   LD/RD         RH/RS      State
192.1.1.2                                        2/13          Up         Up
Session state is UP and not using echo function.
Session Host: Software
OurAddr: 192.1.1.1
Handle: 13
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 750000, MinRxInt: 750000, Multiplier: 3
Received MinRxInt: 750000, Received Multiplier: 15
Holddown (hits): 10772(0), Hello (hits): 750(82985)
Rx Count: 82973, Rx Interval (ms) min/max/avg: 24/1334/659 last: 478 ms ago
Tx Count: 82935, Tx Interval (ms) min/max/avg: 1/1141/660 last: 78 ms ago
Elapsed time watermarks: 0 0 (last: 0)
Registered protocols: Xconnect
Map information:
 Destination[vrf]: 192.1.1.0/24
 Source[vrf]: 192.1.1.1/24
 Template: mh
 Authentication(Type/Keychain): md5/qq
 last_tx_auth_seq: 5  last_rx_auth_seq 4
Uptime: 15:12:26
Last packet: Version: 1                  - Diagnostic: 0
             State bit: Up               - Demand bit: 0
             Poll bit: 0                 - Final bit: 0
             Multiplier: 15              - Length: 48
             My Discr.: 13               - Your Discr.: 2
             Min tx interval: 750000     - Min rx interval: 750000
             Min Echo interval: 0
```

The table below describes the significant fields shown in the displays.

Table 5   *show bfd neighbors* **Field Descriptions for Multihop BFD Sessions**

Field	Description
Destination	The BFD map destination address.
Source	The BFD map source address.
Template	The BFD multihop template name.
Authentication	The authentication type and key chain.
last_tx_auth_seq	The last authenticated sequence sent by the peer.
last_rx_auth_seq	The last authenticated sequence received by the peer.

Related Commands

Command	Description
attach	Connects to a specific line card to execute monitoring and maintenance commands on that line card.

Command	Description
show bfddrops	Displays the number of dropped packets in BFD.
show bfdsummary	Displays summary information for BFD.

show dampening interface

To display a summary of dampened interfaces, use the **showdampinginterface**command in user EXEC or privileged EXEC mode.

show dampening interface commandshow dampening interface

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(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.

Command Examples

The following is sample output from the **showdampinginterface**command in privileged EXEC mode:

```
Router# show dampening interface
3 interfaces are configured with dampening.
No interface is being suppressed.
Features that are using interface dampening:
  IP Routing
  CLNS Routing
```

The table below describes the significant fields shown in the sample output of the show dampening interface command.

Table 6   *show dampening interface Field Descriptions*

Field	Description
... interfaces are configured with dampening.	Displays the number of interfaces that are configured for event dampening.

Field	Description
No interface is being suppressed.	Displays the suppression status of the interfaces that are configured for event dampening.
Features that are using interface dampening:	Displays the routing protocols that are configured to perceived interface dampening.

Related Commands

Command	Description
clear counters	Clears the interface counters.
dampening	Enables IP event dampening at the interface level.
show interface dampening	Displays a summary of the dampening parameters and status.

show interface dampening

To display dampened interfaces on the local router, use the **showinterface** dampening command in privileged EXEC mode.

show interface dampening commandshow interface dampening

Syntax Description

This command has no keywords or arguments.

Command Modes

Privileged EXEC

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.

Command Examples

The following is sample output from the **showinterfacedampening** command:

```
Router# show interface dampening
Flaps Penalty    Supp ReuseTm   HalfL  ReuseV   SuppV  MaxSTm    MaxP Restart
    0        0   FALSE      0        5    1000    2000      20   16000       0
```

The table below describes the significant fields shown in the display.

Table 7   ***show interface dampening Field Descriptions***

Field	Description
Flaps	Displays the number of times that an interface has flapped.

Field	Description
Penalty	Displays the accumulated penalty.
Supp	Indicates if the interface is dampened.
ReuseTm	Displays the reuse timer.
HalfL	Displays the half-life counter.
ReuseV	Displays the reuse threshold timer.
SuppV	Displays the suppress threshold.
MaxSTm	Displays the maximum suppress.
MaxP	Displays the maximum penalty.
Restart	Displays the restart timer.

Related Commands

Command	Description
clear counters	Clears the interface counters.
dampening	Enables IP event dampening at the interface level.
show dampening interface	Displays a summary of interface dampening.

show ip cef platform

To display entries in the Forwarding Information Base (FIB) or to display a summary of the FIB, use the **show ip cef platform**command in privileged EXEC mode.

show ip cef [**ip-prefix** [**mask**]] **platform** [**checksum** | **detail** | **internal checksum**]

Syntax Description		
ip-prefix	(Optional) IP address prefix of the entries to display.
mask	(Optional) Subnet mask of the entries to display.
checksum	(Optional) Displays FIB entry checksum information.
detail	(Optional) Displays detailed FIB entry information.
internal checksum	(Optional) Displays internal data structures. The **checksum** option includes FIB entry checksum information in the output.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	12.2 (28)SB	The command was introduced.
	Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.

Command Examples The following example shows FIB entry information for IP address prefix 10.4.4.4:

```
Router# show ip cef 10.4.4.4 platform

10.4.4.4/32
Fib Entry: 0xD6680610 XCM leaf from 0x50805550(RP) 0xA0805550(FP):
load_bal_or_adj[0] 0x0 load_bal_or_adj[1] 0x18 load_bal_or_adj[2] 0x1C
leaf points to an adjacency, index 0x607
ip_mask 0x0 as_number 0x0 precedence_num_loadbal_intf 0xF0 qos_group 0x0
Label object OCE Chain:
Label(0x12, real) Adjacency
c10k_label_data = 0x450467F8
tag_elt_addr = 0x50003038
ipv6_tag_elt_addr = 0x0
tag_index = 0x607
tt_tag_rew = 0x45046800
Tag Rewrite: vcci = 0x9DA, fib_root = 0x0
```

```
mac_rewrite_index = 0x395, flags = 0x9
pktswitched = 0 byteswitched = 0
XCM Tag Rewrite: vcci = 0x9DA, fib_root = 0x0
mac_rewrite_index = 0x395, flags = 0x9
mac_index_extension = 0x0
XCM mac rewrite from index 0x395
mtu from 0x53800E54(RP) 0xA3800E54(FP)
frag_flags = 0x0
mtu = 1496
mac length 0x12 encap length 0x16 upd_offset=0x02FF
mac string start from bank4 0x32001CA8(RP)
0x82001CA8(FP)
mac string end from bank9 0x50801CA8(RP)
0xA0801CA8(FP)
Encap String: 0005DC387B180003A011A5788100002884700012000
```

The following example shows how to display IP Fast ReRoute (FRR) entry information for IP address prefix 10.4.4.4:

```
Router# show ip cef 10.4.4.4 platform

10.4.4.4/32
=== OCE ===

OCE Type: Fast ReRoute OCE, Number of children: 2
  FRR state: : 1
  FRR next hw oce ptr: : 0x89b002f0
  Backup hw oce ptr: : 0x89b00300
=== OCE ===

OCE Type: Adjacency, Number of children: 0
Adj Type: : IPV4 Adjacency
Encap Len: : 14
L3 MTU: : 1500
Adj Flags: : 0
Fixup Flags: : 0
Interface Name: FastEthernet1/2/7
Encap: : 00 1c b1 d7 8a 44 00 1f 6c 24 30 67 08 00
Next Hop Address: : 0b000002 00000000 00000000 00000000
Next HW OCE Ptr: : 00000000
=== OCE ===

OCE Type: Adjacency, Number of children: 0
Adj Type: : IPV4 Adjacency
Encap Len: : 14
L3 MTU: : 1500
Adj Flags: : 0
Fixup Flags: : 0
Interface Name: FastEthernet1/2/6
Encap: : 00 1c b1 d7 8a 43 00 1f 6c 24 30 66 08 00
Next Hop Address: : 0a000002 00000000 00000000 00000000
Next HW OCE Ptr: : 00000000
```

Related Commands

Command	Description
show cef	Displays which packets the line cards dropped, or displays which packets were not express forwarded.
show cef interface	Displays Cisco Express Forwarding-related interface information.

show ip static route bfd

To display information about the IPv4 static Bidirectional Forwarding Detection (BFD) configuration from specific configured BFD groups and nongroup entries, use the **show ip static route bfd** command in user EXEC or privileged EXEC mode.

show ip static route bfd [**group** [*group-name*]]

Syntax Description

group	(Optional) Specifies a BFD group.
group-name	(Optional) BFD group name.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)S	This command was introduced.

Usage Guidelines

You can specify a BFD group for a set of BFD-tracked static routes. Nongroup entries are BFD-tracked static routes for which a BFD group is not specified. Use the **ip route static bfd** command to configure static route BFD neighbors.

Use the **show ip static route bfd** command to display information about the IPv4 static BFD configuration from specific configured BFD groups and nongroup entries. The **group** *group-name* keyword and argument specifies a BFD group and BFD group name.

Command Examples

The following is sample output from the **show ip static route bfd** command:

```
Router# show ip static route bfd group group1

Codes in []: R - Reachable, U - Unreachable, L - Loop, D - Not Tracked
GigabitEthernet1/1 10.1.1.1 [U] [group1, Active]
GigabitEthernet1/2 10.2.2.2 [U] [group1, Passive]
```

The table below describes the significant fields shown in the display.

Table 8   *show ip static route bfd Field Descriptions*

Field	Description
GigabitEthernet1/1	Interface through which the BFD session is initiated.
10.1.1.1	Next hop IP address.
group1	BFD group name.
Active	Active member of the group.
GigabitEthernet1/2	Interface through which the BFD session is initiated.
10.2.2.2	Next hop IP address.
Passive	Passive member of the group.

Related Commands

Command	Description
ip route static bfd	Specifies static route BFD neighbors.
show ip static route	Displays static route database information.

show ip cache policy

To display the cache entries in the policy route cache, use the **showipcachepolicy**command in EXEC mode.

show ip cache policy commandshow ip cache policy

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

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

Command Examples

The following is sample output from the **showipcachepolicy**command:

```
Router# show ip cache policy
Total adds 10, total deletes 10
Type Routemap/sequence    Age       Interface       Next Hop
NH   george/10            00:04:31  Ethernet0       192.168.1.2
Int  george/30            00:01:23  Serial4         192.168.5.129
```

The table below describes the significant fields shown in the display.

Table 9   show ip cache policy Field Descriptions

Field	Description
Total adds	Number of times a cache entry was created.
total deletes	Number of times a cache entry or the entire cache was deleted.
Type	"NH" indicates the **setipnext-hop** command.
	"Int" indicates the **setinterface**command.

Field	Description
Routemap	Name of the route map that created the entry; in this example, george.
sequence	Route map sequence number.
Age	Age of the cache entry.
Interface	Output interface type and number.
Next Hop	IP address of the next hop.

Related Commands

Command	Description
ip route-cache	Configures the router to export the flow cache entry to a workstation when a flow expires.

show ip local policy

To display the route map used for local policy routing, if any, use the **showiplocalpolicy** command in EXEC mode.

show ip local policy commandshow ip local policy

Syntax Description   This command has no arguments or keywords.

Command Modes   EXEC

Command History

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

Command Examples   The following is sample output from the **showiplocalpolicy** command:

```
Router# show ip local policy
Local policy routing is enabled, using route map equal
route-map equal, permit, sequence 10
  Match clauses:
    length 150 200
  Set clauses:
    ip next-hop 10.10.11.254
  Policy routing matches: 0 packets, 0 bytes
route-map equal, permit, sequence 20
  Match clauses:
    ip address (access-lists): 101
  Set clauses:
    ip next-hop 10.10.11.14
  Policy routing matches: 2 packets, 172 bytes
```

The table below describes the significant fields shown in the display.

Table 10   ***show ip local policy Field Descriptions***

Field	Description
route-map equal	The name of the route map is equal.

Field	Description
permit	The route map contains permit statements.
sequence	The sequence number of the route map, which determines in what order it is processed among other route maps.
Match clauses:	Clauses in the route map that must be matched to satisfy the permit or deny action.
Set clauses:	Set clauses that will be put into place if the match clauses are met.
Policy routing matches: packets	Number of packets that meet the match clauses.
bytes	Number of bytes in the packets that meet the match clauses.

Related Commands

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

show ip policy

To display the route map used for policy routing, use the **showippolicy** command in user EXEC or privileged EXEC mode.

show ip policy

Syntax Description   This command has no arguments or keywords.

Command Modes   User EXEC Privileged EXEC

Command History

Release	Modification
11.1	This command was introduced.
12.3(7)T	The display output was modified to include a label for dynamic route maps.
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.

Command Examples   The following is sample output from the **showippolicy** command:

```
Router# show ip policy
Interface      Route map
local          equal
Ethernet0/2    equal
Ethernet0/3    AAA-02/06/04-14:01:26.619-1-AppSpec (Dynamic)
```

The following is sample output from the **showroute-map** command, which relates to the preceding sample display:

```
Router# show route-map
route-map equal, permit, sequence 10
  Match clauses:
    length 150 200
  Set clauses:
    ip next-hop 10.10.11.254
  Policy routing matches: 0 packets, 0 bytes
route-map equal, permit, sequence 20
  Match clauses:
    ip address (access-lists): 101
  Set clauses:
```

```
       ip next-hop 10.10.11.14
     Policy routing matches: 144 packets, 15190 bytes
```

The table below describes the significant fields shown in the display.

Table 11   show ip policy Field Descriptions

Field	Description
route-map equal	The name of the route map is equal.
permit	The route map contains permit statements.
sequence	Sequence number of the route map, which determines in what order it is processed among other route maps.
Match clauses	Clauses in the route map that must be matched to satisfy the permit or deny action.
Set clauses	Set clauses that will be put into place if the match clauses are met.
Policy routing matches packets	Number of packets that meet the match clauses.
bytes	Number of bytes in the packets that meet the match clauses.

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 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.

show ip protocols

To display the parameters and the current state of the active routing protocol process, use the **showipprotocols** command in privileged EXEC mode.

show ip protocols commandshow ip protocols

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.2(15)T	This command was modified. Support for the route-hold timer was integrated into the output.
12.2(28)SB	This command was integrated into Cisco IOS 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.
15.1(2)S	This command was modified. The output of the command was modified to display that Routing Information Protocol (RIP) default routes are sent on passive interfaces.

Usage Guidelines

The information displayed by the **showipprotocols**command is useful in debugging routing operations. Information in the Routing Information Sources field of the **showipprotocols** output can help you identify a router suspected of delivering bad routing information.

Once you configure the **default-informationoriginateon-passive** command, the output of the **showipprotocols** command displays that RIP default routes are sent on passive interfaces.

Command Examples

The following sample output from the **showipprotocols** command shows Enhanced Interior Gateway Routing Protocol (EIGRP) process 3:

```
Router# show ip protocols
*** IP Routing is NSF aware ***
Routing Protocol is "eigrp 3"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Default networks flagged in outgoing updates
Default networks accepted from incoming updates
Redistributing: eigrp 3
EIGRP-IPv4 VR(test) Address-Family Protocol for AS(3)
Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
NSF-aware route hold timer is 240
Router-ID: 10.1.1.1
Topology : 0 (base)
Active Timer: 3 min
Distance: internal 90 external 170
Maximum path: 4
Maximum hopcount 100
Maximum metric variance 1
Total Prefix Count: 3
Total Redist Count: 0
Automatic Summarization: disabled
Maximum path: 4
Routing for Networks:
10.0.0.0
Routing Information Sources:
Gateway Distance Last Update
10.1.1.2 90 00:05:10
Distance: internal 90 external 170
```

The table below describes the significant fields shown in the display.

Table 12   ***show ip protocols Field Descriptions***

Field	Description
Routing Protocol is...	Name and autonomous system number of the currently running routing protocol.
Outgoing update filter list for all interfaces...	Indicates whether a filter for outgoing routing updates has been specified with the **distribute-listout** command.
Incoming update filter list for all interfaces...	Indicates whether a filter for incoming routing updates has been specified with the **distribute-listin** command.
Redistributing:	Indicates whether route redistribution has been enabled with the **redistribute** command.
EIGRP-IPv4 Protocol for AS(10)	EIGRP instance and autonomous system number.
Metric weight	EIGRP metric calculations.
NSF-aware route hold timer...	Route-hold timer value for a nonstop forwarding (NSF)-aware router.
Router-ID: 10.1.1.1	Router ID.
Topology	Number of entries in the EIGRP topology table.

Field	Description
Active Timer	EIGRP routing active time limit (in minutes).
Distance	Internal and external administrative distance. Internal distance is the degree of preference given to EIGRP internal routes. External distance is the degree of preference given to EIGRP external routes.
Maximum path	Maximum number of parallel routes that the EIGRP can support.
Maximum hopcount	Maximum hop count (in decimal).
Maximum metric variance	Metric variance used to find feasible paths for a route.
Automatic Summarization	Indicates whether route summarization has been enabled with the **auto-summary** command.
Routing for Networks:	Networks for which the routing process is currently injecting routes.
Routing Information Sources:	Lists all the routing sources that the Cisco IOS software is using to build its routing table. The following is displayed for each source: • IP address • Administrative distance • Time the last update was received from this source

Examples

The following sample output from the **showipprotocols** command shows an Intermediate System-to-Intermediate System (IS-IS) process:

```
Router# show ip protocols
Routing Protocol is "isis"
  Sending updates every 0 seconds
  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
  Routing for Networks:
    Serial0
  Routing Information Sources:
  Distance: (default is 115)
```

The table below describes the significant fields shown in the display.

Table 13   *show ip protocols Field Descriptions for an IS-IS Process*

Field	Description
Routing Protocol is "isis"	Specifies the routing protocol used.
Sending updates every 0 seconds	Specifies the time (in seconds) between sending updates.
Invalid after 0 seconds	Specifies the value of the invalid parameter.
hold down 0	Specifies the current value of the hold-down parameter.
flushed after 0	Specifies the time (in seconds) after which the individual routing information will be thrown out (flushed).
Outgoing update ...	Specifies whether the outgoing filtering list has been set.
Incoming update ...	Specifies whether the incoming filtering list has been set.
Redistributing	Lists the protocol that is being redistributed.
Routing	Specifies the networks for which the routing process is currently injecting routes.
Routing Information Sources	Lists all the routing sources the Cisco IOS software is using to build its routing table. For each source, you will see the following displayed: • IP address • Administrative distance • Time the last update was received from this source

Examples   The following sample output from the **showipprotocols** command displays RIP processes:

```
Router# show ip protocols
Routing Protocol is "rip"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Sending updates every 30 seconds, next due in 6 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Sending Default route on Passive interfaces
  Redistributing: rip
  Default version control: send version 2, receive version 2
  Automatic network summarization is not in effect
  Maximum path: 4
  Routing for Networks:
    172.19.0.0
    10.2.0.0
    10.3.0.0
  Passive Interface(s):
    Ethernet0/0
```

```
        Ethernet0/1
        Ethernet0/2
        Ethernet0/3
        Ethernet1/0
        Ethernet1/1
        Ethernet1/2
        Ethernet1/3
     Passive Interface(s):
        Serial2/0
        Serial2/1
        Serial2/2
        Serial2/3
        Serial3/0
        Serial3/1
        Serial3/2
        Serial3/3
     Routing Information Sources:
        Gateway         Distance        Last Update
     Distance: (default is 120)
```

The table below describes the significant fields shown in the display.

Table 14 *show ip protocols Field Descriptions for a RIP Process*

Field	Description
Routing Protocol is "rip"	Specifies the routing protocol used.
Outgoing update ...	Specifies whether the outgoing filtering list has been set.
Incoming update ...	Specifies whether the incoming filtering list has been set.
Sending updates every 30 seconds	Specifies the time (in seconds) between sending updates.
next due in 6 seconds	Specifies when the next update is due to be sent.
Invalid after 180 seconds	Specifies the value of the invalid parameter.
hold down 180	Specifies the current value of the hold-down parameter.
flushed after 240	Specifies the time (in seconds) after which the individual routing information will be thrown (flushed) out.
Sending Default route on Passive interfaces	Specifies that RIP update packets are sent only with a default route on passive interfaces.
Redistributing	Lists the protocol that is being redistributed.
Default version control:	Specifies the version of RIP packets that are sent and received.
Routing	Specifies the networks for which the routing process is currently injecting routes.

Field	Description
Routing Information Sources	Lists all the routing sources the Cisco IOS software is using to build its routing table. For each source, you will see the following displayed: • IP address • Administrative distance • Time the last update was received from this source

Examples

The following is sample output from the **showipprotocols** command. The output shows that the router is running EIGRP, is NSF-aware, and that the route-hold timer is set to 240 seconds, which is the default value for the route-hold timer.

```
Router# show ip protocols
Routing Protocol is "eigrp 101"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 101
  EIGRP NSF-aware route hold timer is 240s
  Automatic network summarization is in effect
  Maximum path: 4
  Routing for Networks:
    10.4.9.0/24
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: internal 90 external 170
```

The table below describes the significant fields shown in the display.

Table 15   *show ip protocols Field Descriptions for an EIGRP NSF-Aware Process*

Field	Description
Routing Protocol is "eigrp 101"	Specifies the routing protocol used.
Outgoing update ...	Specifies whether the outgoing filtering list has been set.
Incoming update ...	Specifies whether the incoming filtering list has been set.
Default networks...	Specifies how these networks will be handled in both incoming and outgoing updates.
EIGRP...	Specifies the value of the K0-K5 metrics, and the maximum hop count.
Redistributing	Lists the protocol that is being redistributed.

Field	Description
EIGRP NSF-Aware...	Displays the route-hold timer value.
Automatic network summarization...	Specifies that automatic summarization is enabled.
Routing	Specifies the networks for which the routing process is currently injecting routes.
Routing Information Sources	Lists all the routing sources the Cisco IOS software is using to build its routing table. For each source, you will see the following displayed: • IP address • Administrative distance • Time the last update was received from this source

Related Commands

Command	Description
auto-summary (EIGRP)	Allows automatic summarization of subnet routes into network-level routes.
default-information originate (RIP)	Generates a default route into RIP.
distribute-list in (IP)	Filters networks received in updates.
distribute-list out (IP)	Suppresses networks from being advertised in updates.
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.

show ip route

To display the current state of the routing table, use the **showiproute** command in user EXEC or privileged EXEC mode.

show ip route [*ip-address* [**repair-paths** | **next-hop-override** [**dhcp**] | *mask* [**longer-prefixes**]] | *protocol* [*process-id*] | **list** [*access-list-number* | *access-list-name*] | **static download** | **update-queue**]

Syntax Description

ip-address	(Optional) IP address about which routing information should be displayed.
repair-paths	(Optional) Displays the repair paths.
next-hop-override	(Optional) Displays the next hop overrides (NHRP) associated with a particular route, along with the corresponding default next hops.
dhcp	(Optional) Displays routes added by the Dynamic Host Configuration Protocol (DHCP) server.
mask	(Optional) The subnet mask.
longer-prefixes	(Optional) Specifies that only routes matching the *ip-address* and *mask* pair should be displayed.
protocol	(Optional) The name of a routing protocol, or the keyword **connected**, **mobile**, **static**, or **summary**. If you specify a routing protocol, use one of the following keywords: **bgp**, **eigrp**, **hello**, **isis**, **odr**, **ospf**, **nhr**, and **rip**.
process-id	(Optional) The number used to identify a process of the specified protocol.
list	(Optional) Filters output by an access list name or number.
access-list-number	(Optional) Specific access list number for which output from the routing table should be displayed.
access-list-name	(Optional) Specific access list name for which output from the routing table should be displayed.
static	(Optional) Displays static routes.
download	(Optional) Displays route installed using the Authentication, Authorization, and Accounting (AAA) route download function. This keyword is used only when AAA is configured.

update-queue	(Optional) Displays Routing Information Base (RIB) queue updates.

Command Modes   User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
9.2	This command was introduced.
10.0	The "D--EIGRP, EX--EIGRP, N1--OSPF NSSA external type 1 route" and "N2--OSPF NSSA external type 2 route" codes were added to the command output.
10.3	The *process-id* argument was added.
11.0	The **longer-prefixes** keyword was added.
11.1	The "U--per-user static route" code was added to the command output.
11.2	The "o--on-demand routing" code was added to the command output.
12.2(33)SRA	This command was modified. The **update-queue** keyword was added.
11.3	The output from the **showiproute***ip-address* command was enhanced to display the origination of an IP route in Intermediate System-to-Intermediate System (IS-IS) networks.
12.0(1)T	The "M--mobile" code was added to the command output.
12.0(3)T	The "P--periodic downloaded static route" code was added to the command output.
12.0(4)T	The "ia--IS-IS" code was added to the command output.
12.2(2)T	The output from the **showiproute***ip-address* command was enhanced to display information on the multipaths to the specified network.
12.2(13)T	The *egp*and *igrp* arguments were removed because the exterior gateway protocol (EGP) and the Interior Gateway Routing Protocol (IGRP) are no longer available in Cisco IOS software.

Release	Modification
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX.
12.3(2)T	The output was enhanced to display route tag information.
12.3(8)T	The output was enhanced to display static routes using DHCP.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRE	This command was modified. The**dhcp** and **repair-paths**keywords were added. Support for the Border Gateway Protocol (BGP) best external and BGP additional path features was added.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was modified. The **next-hop-override**and**nhrp**keywords were added.

Usage Guidelines

The **showiproutestaticdownload**command provides a way to display all dynamic static routes with name and distance information, including active and inactive ones. You can display all active dynamic static routes with both the **showiproute** and **showiproutestatic** commands after these active routes are added in the main routing table.

Command Examples

Examples

The following examples show the standard routing tables displayed by the **showiproute** command. Use the codes displayed at the beginning of each report and the information in the table below to understand the type of route.

The following is sample output from the**showiproute** command when entered without an address:

```
Router# show ip route
Codes: R - RIP derived, O - OSPF derived,
       C - connected, S - static, B - BGP derived,
       * - candidate default route, IA - OSPF inter area route,
       i - IS-IS derived, ia - IS-IS, U - per-user static route,
       o - on-demand routing, M - mobile, P - periodic downloaded static route,
       D - EIGRP, EX - EIGRP external, E1 - OSPF external type 1 route,
```

```
          E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
          N2 - OSPF NSSA external type 2 route
Gateway of last resort is 10.119.254.240 to network 10.140.0.0
O E2 10.110.0.0 [160/5] via 10.119.254.6, 0:01:00, Ethernet2
E    10.67.10.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
O E2 10.68.132.0 [160/5] via 10.119.254.6, 0:00:59, Ethernet2
O E2 10.130.0.0 [160/5] via 10.119.254.6, 0:00:59, Ethernet2
E    10.128.0.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E    10.129.0.0 [200/129] via 10.119.254.240, 0:02:22, Ethernet2
E    10.65.129.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E    10.10.0.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E    10.75.139.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
E    10.16.208.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E    10.84.148.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
E    10.31.223.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E    10.44.236.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
E    10.141.0.0 [200/129] via 10.119.254.240, 0:02:22, Ethernet2
E    10.140.0.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
```

The following is sample output that includes IS-IS Level 2 routes learned:

```
Router# show ip route
Codes: R - RIP derived, O - OSPF derived,
       C - connected, S - static, B - BGP derived,
       * - candidate default route, IA - OSPF inter area route,
       i - IS-IS derived, ia - IS-IS, U - per-user static route,
       o - on-demand routing, M - mobile, P - periodic downloaded static route,
       D - EIGRP, EX - EIGRP external, E1 - OSPF external type 1 route,
       E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
       N2 - OSPF NSSA external type 2 route
Gateway of last resort is not set
     10.89.0.0 is subnetted (mask is 255.255.255.0), 3 subnets
C       10.89.64.0 255.255.255.0 is possibly down,
          routing via 0.0.0.0, Ethernet0
i L2    10.89.67.0 [115/20] via 10.89.64.240, 0:00:12, Ethernet0
i L2    10.89.66.0 [115/20] via 10.89.64.240, 0:00:12, Ethernet0
```

The following is sample output using the **longer-prefixes** keyword. When the **longer-prefixes** keyword is included, the address and mask pair becomes the prefix, and any address that matches that prefix is displayed. Therefore, multiple addresses are displayed.

In the following example, the logical AND operation is performed on the source address 10.0.0.0 and the mask 10.0.0.0, resulting in 10.0.0.0. Each destination in the routing table is also logically ANDed with the mask and compared to that result of 10.0.0.0. Any destinations that fall into that range are displayed in the output.

```
Router# show ip route 10.0.0.0 10.0.0.0 longer-prefixes

Codes: R - RIP derived, O - OSPF derived,
       C - connected, S - static, B - BGP derived,
       * - candidate default route, IA - OSPF inter area route,
       i - IS-IS derived, ia - IS-IS, U - per-user static route,
       o - on-demand routing, M - mobile, P - periodic downloaded static route,
       D - EIGRP, EX - EIGRP external, E1 - OSPF external type 1 route,
       E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
       N2 - OSPF NSSA external type 2 route

Gateway of last resort is not set

S    10.134.0.0 is directly connected, Ethernet0
S    10.10.0.0 is directly connected, Ethernet0
S    10.129.0.0 is directly connected, Ethernet0
S    10.128.0.0 is directly connected, Ethernet0
S    10.49.246.0 is directly connected, Ethernet0
S    10.160.97.0 is directly connected, Ethernet0
S    10.153.88.0 is directly connected, Ethernet0
S    10.76.141.0 is directly connected, Ethernet0
S    10.75.138.0 is directly connected, Ethernet0
S    10.44.237.0 is directly connected, Ethernet0
S    10.31.222.0 is directly connected, Ethernet0
S    10.16.209.0 is directly connected, Ethernet0
```

```
S    10.145.0.0 is directly connected, Ethernet0
S    10.141.0.0 is directly connected, Ethernet0
S    10.138.0.0 is directly connected, Ethernet0
S    10.128.0.0 is directly connected, Ethernet0
     10.19.0.0 255.255.255.0 is subnetted, 1 subnets
C       10.19.64.0 is directly connected, Ethernet0
     10.69.0.0 is variably subnetted, 2 subnets, 2 masks
C       10.69.232.32 255.255.255.240 is directly connected, Ethernet0
S       10.69.0.0 255.255.0.0 is directly connected, Ethernet0
```

The following examples display all downloaded static routes. A P designates which route was installed using AAA route download.

```
Router# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR, P - periodic downloaded static route
       T - traffic engineered route

Gateway of last resort is 172.21.17.1 to network 0.0.0.0

        172.31.0.0/32 is subnetted, 1 subnets
P       172.31.229.41 is directly connected, Dialer1 20.0.0.0/24 is subnetted, 3 subnets
P       10.1.1.0 [200/0] via 172.31.229.41, Dialer1
P       10.1.3.0 [200/0] via 172.31.229.41, Dialer1
P       10.1.2.0 [200/0] via 172.31.229.41, Dialer1
Router# show ip route static
     172.27.4.0/8 is variably subnetted, 2 subnets, 2 masks
P       172.16.1.1/32 is directly connected, BRI0
P       172.27.4.0/8 [1/0] via 10.1.1.1, BRI0
S    172.31.0.0/16 [1/0] via 172.21.114.65, Ethernet0
S    10.0.0.0/8 is directly connected, BRI0
P    10.0.0.0/8 is directly connected, BRI0
     172.21.0.0/16 is variably subnetted, 5 subnets, 2 masks
S       172.21.114.201/32 is directly connected, BRI0
S       172.21.114.205/32 is directly connected, BRI0
S       172.21.114.174/32 is directly connected, BRI0
S       172.21.114.12/32 is directly connected, BRI0
P    10.0.0.0/8 is directly connected, BRI0
P    10.1.0.0/16 is directly connected, BRI0
P    10.2.2.0/24 is directly connected, BRI0
S*   0.0.0.0/0 [1/0] via 172.21.114.65, Ethernet0
S    172.29.0.0/16 [1/0] via 172.21.114.65, Ethernet0
```

The following example shows how to use the **showiproutestaticdownload** command to display all active and inactive routes installed using AAA route download:

```
Router# show ip route static download
Connectivity: A - Active, I - Inactive

A    10.10.0.0 255.0.0.0 BRI0
A    10.11.0.0 255.0.0.0 BRI0
A    10.12.0.0 255.0.0.0 BRI0
A    10.13.0.0 255.0.0.0 BRI0
I    10.20.0.0 255.0.0.0 172.21.1.1
I    10.22.0.0 255.0.0.0 Serial0
I    10.30.0.0 255.0.0.0 Serial0
I    10.31.0.0 255.0.0.0 Serial1
I    10.32.0.0 255.0.0.0 Serial1
A    10.34.0.0 255.0.0.0 192.168.1.1
A    10.36.1.1 255.255.255.255 BRI0 200 name remote1
I    10.38.1.9 255.255.255.0 192.168.69.1
```

The following example shows how to use the **showiproutenhrp** command to enable shortcut switching on the tunnel interface:

```
Router# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
```

```
                  D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
                  N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
                  E1 - OSPF external type 1, E2 - OSPF external type 2
                  i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
                  ia - IS-IS inter area, * - candidate default, U - per-user static route
                  o - ODR, P - periodic downloaded static route, H - NHRP
Gateway of last resort is not set
10.0.0.0/16 is variably subnetted, 3 subnets, 2 masks
C       10.1.1.0/24 is directly connected, Tunnel0
C       172.16.22.0 is directly connected, Ethernet1/0
H       172.16.99.0 [250/1] via 10.1.1.99, 00:11:43, Tunnel0
     10.11.0.0/24 is subnetted, 1 subnets
C       10.11.11.0 is directly connected, Ethernet0/0
Router# show ip route nhrp
H       172.16.99.0 [250/1] via 10.1.1.99, 00:11:43, Tunnel0
```

The following is sample output using the **next-hop-override** keyword. When the **next-hop-override** keyword is included, the NHRP Nexthop-overrides associated with a particular route, along with the corresponding default next hops, are displayed.

```
================================================================
1) Initial configuration
================================================================
Router# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route

Gateway of last resort is not set
     10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       10.2.1.0/24 is directly connected, Loopback1
L       10.2.1.1/32 is directly connected, Loopback1
     10.0.0.0/24 is subnetted, 1 subnets
S       10.10.10.0 is directly connected, Tunnel0
     10.11.0.0/24 is subnetted, 1 subnets
S       10.11.11.0 is directly connected, Ethernet0/0
Router# show ip route next-hop-override
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route

Gateway of last resort is not set
     10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       10.2.1.0/24 is directly connected, Loopback1
L       10.2.1.1/32 is directly connected, Loopback1
     10.0.0.0/24 is subnetted, 1 subnets
S       10.10.10.0 is directly connected, Tunnel0
     10.11.0.0/24 is subnetted, 1 subnets
S       10.11.11.0 is directly connected, Ethernet0/0
Router# show ip cef
Prefix               Next Hop            Interface
.
.
.
10.2.1.255/32         receive             Loopback1
10.10.10.0/24         attached            Tunnel0  <<<<<<<<
10.11.11.0/24         attached            Ethernet0/0
127.0.0.0/8           drop
.
.
.
================================================================
```

```
2) Add a Nexthop-override
   address = 10.10.10.0
   mask = 255.255.255.0
   gateway = 10.1.1.1
   interface = Tunnel0
================================================================
Router# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route

Gateway of last resort is not set
       10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C         10.2.1.0/24 is directly connected, Loopback1
L         10.2.1.1/32 is directly connected, Loopback1
       10.0.0.0/24 is subnetted, 1 subnets
% S       10.10.10.0 is directly connected, Tunnel0
       10.11.0.0/24 is subnetted, 1 subnets
S         10.11.11.0 is directly connected, Ethernet0/0

Router# show ip route next-hop-override
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route

Gateway of last resort is not set
       10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C         10.2.1.0/24 is directly connected, Loopback1
L         10.2.1.1/32 is directly connected, Loopback1
       10.0.0.0/24 is subnetted, 1 subnets
% S       10.10.10.0 is directly connected, Tunnel0
                    [NHO][1/0] via 10.1.1.1, Tunnel0
       10.11.0.0/24 is subnetted, 1 subnets
S         10.11.11.0 is directly connected, Ethernet0/0

Router# show ip cef
Prefix                Next Hop              Interface
.
.
.
10.2.1.255/32         receive               Loopback110.10.10.0/24

10.10.10.0/24         10.1.1.1              Tunnel0
10.11.11.0/24         attached              Ethernet0/0
10.12.0.0/16 drop
.
.
.
================================================================
3) Delete a Nexthop-override
   address = 10.10.10.0
   mask = 255.255.255.0
   gateway = 10.11.1.1
   interface = Tunnel0
================================================================
Router# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
```

```
            + - replicated route

Gateway of last resort is not set
       10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        10.2.1.0/24 is directly connected, Loopback1
L        10.2.1.1/32 is directly connected, Loopback1
       10.0.0.0/24 is subnetted, 1 subnets
S        10.10.10.0 is directly connected, Tunnel0
       10.11.0.0/24 is subnetted, 1 subnets
S        10.11.11.0 is directly connected, Ethernet0/0

Router# show ip route next-hop-override
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route

Gateway of last resort is not set
       10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        10.2.1.0/24 is directly connected, Loopback1
L        10.2.1.1/32 is directly connected, Loopback1
       10.0.0.0/24 is subnetted, 1 subnets
S        10.10.10.0 is directly connected, Tunnel0
       10.11.0.0/24 is subnetted, 1 subnets
S        10.11.11.0 is directly connected, Ethernet0/0

Router# show ip cef
Prefix              Next Hop          Interface
.
.
.
10.2.1.255/32        receive              Loopback110.10.10.0/24

10.10.10.0/24        attached             Tunnel0
10.11.11.0/24        attached          Ethernet0/0
10.120.0.0/16 drop
.
.
.
```

Table 16 ***show ip route Field Descriptions***

Field	Description
Codes	Indicates the protocol that derived the route. It can be one of the following values: • B-- BGP derived • C--connected • D--Enhanced Interior Gateway Routing Protocol (EIGRP) • EX--EIGRP external • H-- NHRP • i--IS-IS derived • ia--IS-IS • L--local • M--mobile • O--Open Shortest Path First (OSPF) derived • P--periodic downloaded static route • R--Routing Information Protocol (RIP) derived • S--static • U--per-user static route • o--on-demand routing • +--replicated route
Codes	Type of route. It can be one of the following values: *--Indicates the last path used when a packet was forwarded. It pertains only to the nonfast-switched packets. However, it does not indicate which path will be used next when forwarding a nonfast-switched packet, except when the paths are equal cost. • E1--OSPF external type 1 route • E2--OSPF external type 2 route • IA--OSPF inter area route • L1--IS-IS Level 1 route • L2--IS-IS Level 2 route • N1--OSPF not-so-stubby area (NSSA) external type 1 route • N2--OSPF NSSA external type 2 route
10.110.0.0	Indicates the address of the remote network.
[160/5]	The first number in the brackets is the administrative distance of the information source; the second number is the metric for the route.

Field	Description
via 10.119.254.6	Specifies the address of the next router to the remote network.
0:01:00	Specifies the last time the route was updated (in hours:minutes:seconds).
Ethernet2	Specifies the interface through which the specified network can be reached.

Examples

When you specify that you want information about a specific network displayed, more detailed statistics are shown. The following is sample output from the **showiproute** command when entered with the IP address 10.0.0.1:

```
Router# show ip route 10.0.0.1
Routing entry for 10.0.0.1/32
    Known via "isis", distance 115, metric 20, type level-1
    Redistributing via isis
    Last update from 10.191.255.251 on Fddi1/0, 00:00:13 ago
    Routing Descriptor Blocks:
  * 10.22.22.2, from 10.191.255.247, via Serial2/3
      Route metric is 20, traffic share count is 1
      10.191.255.251, from 10.191.255.247, via Fddi1/0
      Route metric is 20, traffic share count is 1
```

When an IS-IS router advertises its link-state information, it includes one of its own IP addresses to be used as the originator IP address. When other routers calculate IP routes, they can store the originator IP address with each route in the routing table.

The preceding example shows the output from the **showiproute** command for an IP route generated by IS-IS. Each path that is shown under the Routing Descriptor Blocks report displays two IP addresses. The first address (10.22.22.2) is the next hop address. The second is the originator IP address from the advertising IS-IS router. This address helps you determine where a particular IP route has originated in your network. In the example the route to 10.0.0.1/32 was originated by a router with IP address 10.191.255.247.

The table below describes the significant fields shown when using the **showiproute** command with an IP address.

Table 17   show ip route with IP Address Field Descriptions

Field	Description
Routing entry for 10.0.0.1/32	Network number and mask.
Known via...	Indicates how the route was derived.
Tag	Integer that is used to implement the route.
type	Indicates the IS-IS route type (Level 1 or Level 2).
Redistributing via...	Indicates the redistribution protocol.

Field	Description
Last update from 10.191.255.251	Indicates the IP address of a router that is the next hop to the remote network and the router interface on which the last update arrived.
Routing Descriptor Blocks:	Displays the next hop IP address followed by the information source.
Route metric	This value is the best metric for this routing descriptor block.
traffic share count	Number of uses for this routing descriptor block.

The following is sample output using the **longer-prefixes** keyword. When the **longer-prefixes** keyword is included, the address and mask pair becomes the prefix, and any address that matches that prefix is displayed. Therefore, multiple addresses are displayed.

In the following example, the logical AND operation is performed on the source address 10.0.0.0 and the mask 10.0.0.0, resulting in 10.0.0.0. Each destination in the routing table is also logically ANDed with the mask and compared to that result of 10.0.0.0. Any destinations that fall into that range are displayed in the output.

```
Router# show ip route 10.0.0.0 10.0.0.0 longer-prefixes

Codes: R - RIP derived, O - OSPF derived,
       C - connected, S - static, B - BGP derived,
       * - candidate default route, IA - OSPF inter area route,
       i - IS-IS derived, ia - IS-IS, U - per-user static route,
       o - on-demand routing, M - mobile, P - periodic downloaded static route,
       D - EIGRP, EX - EIGRP external, E1 - OSPF external type 1 route,
       E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
       N2 - OSPF NSSA external type 2 route

Gateway of last resort is not set

S    10.134.0.0 is directly connected, Ethernet0
S    10.10.0.0 is directly connected, Ethernet0
S    10.129.0.0 is directly connected, Ethernet0
S    10.128.0.0 is directly connected, Ethernet0
S    10.49.246.0 is directly connected, Ethernet0
S    10.160.97.0 is directly connected, Ethernet0
S    10.153.88.0 is directly connected, Ethernet0
S    10.76.141.0 is directly connected, Ethernet0
S    10.75.138.0 is directly connected, Ethernet0
S    10.44.237.0 is directly connected, Ethernet0
S    10.31.222.0 is directly connected, Ethernet0
S    10.16.209.0 is directly connected, Ethernet0
S    10.145.0.0 is directly connected, Ethernet0
S    10.141.0.0 is directly connected, Ethernet0
S    10.138.0.0 is directly connected, Ethernet0
S    10.128.0.0 is directly connected, Ethernet0
     10.19.0.0 255.255.255.0 is subnetted, 1 subnets
C       10.19.64.0 is directly connected, Ethernet0
     10.69.0.0 is variably subnetted, 2 subnets, 2 masks
C       10.69.232.32 255.255.255.240 is directly connected, Ethernet0
S       10.69.0.0 255.255.0.0 is directly connected, Ethernet0
```

The following output includes the tag 120 applied to the route 10.22.0.0/16. You must specify an IP prefix in order to see the tag value.

```
Router# show ip route 10.22.0.0
Routing entry for 10.22.0.0/16
  Known via "isis", distance 115, metric 12
  Tag 120, type level-1
```

```
          Redistributing via isis
          Last update from 172.19.170.12 on Ethernet2, 01:29:13 ago
          Routing Descriptor Blocks:
            * 172.19.170.12, from 10.3.3.3, via Ethernet2
                Route metric is 12, traffic share count is 1
                Route tag 120
```

Examples

The following example shows that IP route 10.8.8.0 is directly connected to the Internet and is the next-hop (option 3) default gateway. Routes 10.1.1.1 [1/0], 10.3.2.1 [24/0], and 172.2.2.2 [1/0] are static, and route 10.0.0.0/0 is a default route candidate.

```
Router# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is 10.0.19.14 to network 0.0.0.0
10.0.0.0/24 is subnetted, 1 subnets
C 10.8.8.0 is directly connected, Ethernet1
  10.0.0.0/32 is subnetted, 1 subnets
S 10.1.1.1 [1/0] via 10.8.8.1
  10.0.0.0/32 is subnetted, 1 subnets
S 10.3.2.1 [24/0] via 10.8.8.1
  172.16.0.0/32 is subnetted, 1 subnets
S 172.2.2.2 [1/0] via 10.8.8.1
  10.0.0.0/28 is subnetted, 1 subnets
C 10.0.19.0 is directly connected, Ethernet0
  10.0.0.0/24 is subnetted, 1 subnets
C 10.15.15.0 is directly connected, Loopback0
S* 10.0.0.0/0 [1/0] via 10.0.19.14
```

The following sample output from the **showiprouterepair-paths** command shows the repair paths marked with the tag [RPR]:

```
Router# show ip route repair-paths
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/32 is subnetted, 3 subnets
C       10.1.1.1 is directly connected, Loopback0
B       10.2.2.2 [200/0] via 172.16.1.2, 00:31:07
                [RPR][200/0] via 192.168.1.2, 00:31:07
B       10.9.9.9 [20/0] via 192.168.1.2, 00:29:45
                [RPR][20/0] via 192.168.3.2, 00:29:45
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.1.0/24 is directly connected, Ethernet0/0
L       172.16.1.1/32 is directly connected, Ethernet0/0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, Serial2/0
L       192.168.1.1/32 is directly connected, Serial2/0
B     192.168.3.0/24 [200/0] via 172.16.1.2, 00:31:07
                     [RPR][200/0] via 192.168.1.2, 00:31:07
B     192.168.9.0/24 [20/0] via 192.168.1.2, 00:29:45
                     [RPR][20/0] via 192.168.3.2, 00:29:45
B     192.168.13.0/24 [20/0] via 192.168.1.2, 00:29:45
                      [RPR][20/0] via 192.168.3.2, 00:29:45
Router# show ip route repair-paths 10.9.9.9
```

```
>Routing entry for 10.9.9.9/32
>  Known via "bgp 100", distance 20, metric 0
>  Tag 10, type external
>  Last update from 192.168.1.2 00:44:52 ago
>  Routing Descriptor Blocks:
>  * 192.168.1.2, from 192.168.1.2, 00:44:52 ago, recursive-via-conn
>      Route metric is 0, traffic share count is 1
>      AS Hops 2
>      Route tag 10
>      MPLS label: none
>    [RPR]192.168.3.2, from 172.16.1.2, 00:44:52 ago
>      Route metric is 0, traffic share count is 1
>      AS Hops 2
>      Route tag 10
>      MPLS label: none
```

Related Commands

Command	Description
show dialer	Displays general diagnostic information for interfaces configured for DDR.
show interfaces tunnel	Displays a list of tunnel interface information.
show ip route summary	Displays the current state of the routing table in summary format.

show ip route loops

To display all routes currently in the routing information base (RIB) that are part of a loop, use the **showiprouteloops** command in user EXEC or privileged EXEC mode.

show ip route loops

Syntax Description   This command has no arguments or keywords.

Command Modes   User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines   Use the **showiprouteloops** command to display information about all routes currently in the RIB that are part of a loop.

For example, the following configuration introduces a loop in the RIB that cannot be safely resolved without the risk of oscillation.

```
ip route 0.0.0.0 0.0.0.0 192.168.5.6
ip route 192.168.0.0 255.255.0.0 192.168.1.2
```

Note   The above configuration is not useful. The same forwarding behavior can be achieved if you configure **iproute0.0.0.00.0.0.0192.168.1.2**.

When the connected route for 192.168.1.2/30 is removed, loop is introduced and the following log message is displayed:

```
*Mar 31 15:50:16.307: %IPRT-3-RIB_LOOP: Resolution loop formed by routes in RIB
```

You can use the **showiprouteloops** command to view information about this loop.

Command Examples   The following is sample output from the **showiprouteloops** command. The fields are self-explanatory.

```
Router# show ip route loops
default:ipv4:base 192.168.0.0/16 -> base 192.168.1.2 static 00:56:46
default:ipv4:base 0.0.0.0/0 -> base 192.168.5.6 static 00:56:46 N
```

Related Commands

Command	Description
ip route	Establishes static routes.

show ip route profile

To display routing table change statistics, use the **showiprouteprofile** command in EXEC mode.

sshow ip route profile commandhow ip route profile

Syntax Description   This command has no arguments or keywords.

Command Default   No default behavior or values

Command Modes   EXEC

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   Use this command in combination with the **iprouteprofile** global configuration command to validate the routing table change statistics.

Command Examples   The following example shows the frequency of routing table changes in a 5-second sampling interval. In this example, the Prefix add change occurred 22 times in one interval and 24 times in another interval. The output represents this with a Fwd-path change value of 2 and a Prefix add value of 2:

```
Router# show ip route profile
-----------------------------------------------------------------
Change/     Fwd-path    Prefix     Nexthop     Pathcount    Prefix
interval    change      add        Change      Change       refresh
-----------------------------------------------------------------
0           87          87         89          89           89
1           0           0          0           0            0
2           0           0          0           0            0
3           0           0          0           0            0
4           0           0          0           0            0
5           0           0          0           0            0
```

```
10           0           0           0           0           0
15           0           0           0           0           0
20           2           2           0           0           0
25           0           0           0           0           0
```

The table below describes the significant fields shown in the display.

Table 18   *show ip route profile Field Descriptions*

Field	Description
Change/interval	Represents the frequency buckets. A Change/interval of 20 represents the bucket that is incremented when a particular event occurs 20 times in a sampling interval. It is very common to see high counters for the Change/interval bucket for 0. This counter represents the number of sampling intervals in which there were no changes to the routing table. Route removals are not counted in the statistics, only route additions.
Fwd-path change	Number of changes in the forwarding path. This value represents the accumulation of Prefix add, Nexthop change, and Pathcount change.
Prefix add	A new prefix was added to the routing table.
Nexthop 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 change is the result of an increase in the number of paths for an Interior Gateway Protocol (IGP).
Prefix refresh	Indicates standard routing table maintenance. The forwarding behavior was not changed.

Related Commands

Command	Description
ip route profile	Enables IP routing table statistics collection

show ip route summary

To display the current state of the routing table, use the **showiproutesummary** command in privileged EXEC mode.

shshow ip route summary commandow ip route summary

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.3(2)T	The number of multipaths supported by the routing table was added to the output.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Command Examples

The following is sample output from the **showiproutesummary** command:

```
Router# show ip route summary
IP routing table name is Default-IP-Routing-Table(0)
IP routing table maximum-paths is 16
Route Source    Networks    Subnets    Overhead    Memory (bytes)
connected       0           3          126         360
static          1           2          126         360
eigrp 109       747         12         31878       91080
internal        3                                  360
Total           751         17         32130       92160
```

describes the significant fields shown in the display.

Table 19   ***show ip route summary Field Descriptions***

Field	Description
IP routing table name is...	Displays routing table type and table ID.
IP routing table maximum-paths is...	Number of parallel routes supported by this routing table.
Route Source	Routing protocol name, or the **connected,static,** or **internal**keyword. "Internal" indicates those routes that are in the routing table that are not owned by any routing protocol.
Networks	Number of prefixes that are present in the routing table for each route source.
Subnets	Number of subnets that are present in the routing table for each route source, including host routes.
Overhead	Any additional memory involved in allocating the routes for the particular route source other than the memory specified in the Memory field.
Memory	Number of bytes allocated to maintain all the routes for the particular route source.

show ip route supernets-only

To display information about supernets, use the **showiproutesupernets-only** command in privileged EXEC mode.

show ip route supernets-only commandshow ip route supernets-only

Syntax Description   This command has no arguments or keywords.

Command Modes   Privileged EXEC

Command History

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

Command Examples   The following is sample output from the **showiproutesupernets-only** command. This display shows supernets only; it does not show subnets.

```
Router# show ip route supernets-only
Codes: R - RIP derived, O - OSPF derived
       C - connected, S - static, B - BGP derived
       i - IS-IS derived, D - EIGRP derived
       * - candidate default route, IA - OSPF inter area route
       E1 - OSPF external type 1 route, E2 - OSPF external type 2 route
       L1 - IS-IS level-1 route, L2 - IS-IS level-2 route
       EX - EIGRP external route
Gateway of last resort is not set
B    172.16.0.0 (mask is 255.255.0.0) [20/0] via 172.16.72.30, 0:00:50
B    192.0.0.0 (mask is 255.0.0.0) [20/0] via 172.16.72.24, 0:02:50
```

The table below describes the significant fields shown in the display.

Table 20   *show ip route supernets-only Field Descriptions*

Field	Description
B	Border Gateway Protocol (BGP) derived, as shown in list of codes.

Field	Description
172.16.0.0 (mask is 255.255.0.0)	Supernet IP address.
[20/0]	Administrative distance (external/internal).
via 172.16.72.30	Next hop IP address.
0:00:50	Age of the route (how long ago the update was received).

show ip route track-table

To display information about the IP route track table, use the **showiproutetrack-table** command in privileged EXEC mode.

> **show ip route track-table**

Syntax Description   This command has no arguments or keywords.

Command Modes   Privileged EXEC (#)

Command History

Release	Modification
12.3(2)XE	This command was introduced.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Command Examples   The following example displays information about the IP route track table:

```
Router# show ip route track-table
ip route 0.0.0.0 0.0.0.0 10.1.1.242 track-object 123 state is [up]
```

The table below describes the significant fields shown in the display.

Table 21   show ip route track-table Field Descriptions

Field	Description
ip route	The configured IP route.
track-object	The track object number.
state is	The state of the track object. The object may be up or down.

Related Commands

Command	Description
ip route	Establishes static routes in a required network.

show ip static route

To display the static process local Routing Information Base (RIB) information, use the **showipstaticroute**command in user EXEC or privileged EXEC configuration mode.

show ip static route [**bfd**] [**vrf** *vrf-name*] [**topology** *topology-name*] [*ip-address* [*mask*]] [**multicast**] [**summary**]

Syntax Description

bfd	(Optional) Displays IPv4 static Bidirectional Forwarding Detection (BFD) neighbor information.
vrf *vrf-name*	(Optional) Name of the VRF by which static routing information should be displayed.
topology *topology-name*	(Optional) Static route information for the specified topology.
ip-address	(Optional) Address by which static routing information should be displayed.
mask	(Optional) Subnet mask.
multicast	(Optional) Displays IPv4 multicast information.
summary	(Optional) Displays summary information.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.2(33)SRC	The command output was enhanced to include BFD neighbor information.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Command Examples

The following is sample output from the **showipstaticroute** command:

```
Router# show ip static route
Codes: M - Manual static, A - AAA download, N - IP NAT, D - DHCP,
       G - GPRS, V - Crypto VPN, C - CASA, P - Channel interface processor,
       B - BootP, S - Service selection gateway
       DN - Default Network, T - Tracking object
```

```
      L - TL1, E - OER
Codes in []: A - active, N - non-active, B - BFD-tracked, P - permanent
```

The table below describes the significant fields shown in the display.

Table 22   *show ip static route Descriptions*

Field	Description
Codes	Indicates the protocol that derived the route. The status codes are defined in the output.

show ip static route bfd

To display information about the IPv4 static Bidirectional Forwarding Detection (BFD) configuration from specific configured BFD groups and nongroup entries, use the **show ip static route bfd** command in user EXEC or privileged EXEC mode.

show ip static route bfd [**group** [*group-name*]]

Syntax Description

group	(Optional) Specifies a BFD group.
group-name	(Optional) BFD group name.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)S	This command was introduced.

Usage Guidelines

You can specify a BFD group for a set of BFD-tracked static routes. Nongroup entries are BFD-tracked static routes for which a BFD group is not specified. Use the **ip route static bfd** command to configure static route BFD neighbors.

Use the **show ip static route bfd** command to display information about the IPv4 static BFD configuration from specific configured BFD groups and nongroup entries. The **group** *group-name* keyword and argument specifies a BFD group and BFD group name.

Command Examples

The following is sample output from the **show ip static route bfd** command:

```
Router# show ip static route bfd group group1

Codes in []: R - Reachable, U - Unreachable, L - Loop, D - Not Tracked
GigabitEthernet1/1 10.1.1.1 [U] [group1, Active]
GigabitEthernet1/2 10.2.2.2 [U] [group1, Passive]
```

The table below describes the significant fields shown in the display.

Table 23 *show ip static route bfd Field Descriptions*

Field	Description
GigabitEthernet1/1	Interface through which the BFD session is initiated.
10.1.1.1	Next hop IP address.
group1	BFD group name.
Active	Active member of the group.
GigabitEthernet1/2	Interface through which the BFD session is initiated.
10.2.2.2	Next hop IP address.
Passive	Passive member of the group.

Related Commands

Command	Description
ip route static bfd	Specifies static route BFD neighbors.
show ip static route	Displays static route database information.

show isis fast-reroute

To display information about Intermediate System-to-Intermediate System (IS-IS) Fast Reroute (FRR) configurations, use the **show isis fast-reroute** command in user EXEC or privileged EXEC mode.

show isis fast-reroute {**interfaces** [*type number*] | **summary**}

Syntax Description

interfaces	Displays information about all interfaces that are configured with FRR.
type	(Optional) Interface type. For more information, use the question mark (?) online help function.
number	(Optional) Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
summary	Displays FRR configuration information summary.

Command Default

This command has no default settings.

Command Modes

User EXEC (>) Privileged EXEC (#)

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

The **show isis fast-reroute interfaces** command displays whether or not an interface is supported by a platform.

Command Examples

The following is sample output from the **show isis fast-reroute interfaces** command:

```
Router# show isis fast-reroute interfaces
Tag Null - Fast-Reroute Platform Support Information:
    Serial6/3: Protectable: Yes. Usable for repair: Yes
```

```
Serial6/2: Protectable: Yes. Usable for repair: Yes
Loopback16: Protectable: No. Usable for repair: No
```

The table below describes the significant fields shown in the display.

Table 24   *show isis fast-reroute interfaces Field Descriptions*

Field	Description
Protectable	Specifies whether or not an interface is a protected interface.
Usable for repair	Specifies whether or not an interface can be used as a repair path.

The following is sample output from the **show isis fast-reroute summary** command:

```
Router# show isis fast-reroute summary

Prefix Counts:        Total      Protected    Coverage
  High priority:       17          17           100%
  Normal priority:     0           0            0%
```

The table below describes the significant fields shown in the display.

Table 25   *show isis fast-reroute summary Field Descriptions*

Field	Description
Total	Total number of prefixes.
Protected	Total number of protected prefixes.
High priority	Prefixes that have a high priority.
Normal priority	Prefixes that have a normal priority.

Related Commands

Command	Description
debug isis fast-reroute	Enables debugging of IS-IS FRR.
fast-reroute load-sharing	Disables FRR load sharing of prefixes.
fast-reroute per-prefix	Enables FRR per prefix.
fast-reroute tie-break	Configures the FRR tiebreaking priority.

show key chain

To display authentication key information, use the **showkeychain** command in EXEC mode.

show key chain commandshow key chain [*name-of-chain*]

Syntax Description

name-of-chain	(Optional) Name of the key chain to display, as named in the **keychain** command.

Command Default

Information about all key chains is displayed.

Command Modes

EXEC

Command History

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

Command Examples

The following is sample output from the **showkeychain** command:

```
Router# show key chain
Key-chain trees:
    key 1 -- text "chestnut"
        accept lifetime (always valid) - (always valid) [valid now]
        send lifetime (always valid) - (always valid) [valid now]
    key 2 -- text "birch"
        accept lifetime (00:00:00 Dec 5 1995) - (23:59:59 Dec 5 1995)
        send lifetime (06:00:00 Dec 5 1995) - (18:00:00 Dec 5 1995)
```

Related Commands

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

show monitor event-trace

To display event trace messages for Cisco IOS software subsystem components, use the **showmonitorevent-trace** command in privileged EXEC mode.

> **show monitor event-trace**[*all-traces*] [*component* {**all** | **back** *hour:minute* | **clock** *hour:minute* | **from-boot** *seconds* | **latest** | **parameters**}

Syntax Description

all-traces	(Optional) Displays all event trace messages in memory to the console.
component	(Optional) Name of the Cisco IOS software subsystem component that is the object of the event trace. To get a list of components that support event tracing in this release, use the **monitorevent-trace?** command.
all	Displays all event trace messages currently in memory for the specified component.
back *hour:minute*	Specifies how far back from the current time you want to view messages. For example, you can gather messages from the last 30 minutes. The time argument is specified in hours and minutes format (hh:mm).
clock *hour:minute*	Displays event trace messages starting from a specific clock time in hours and minutes format (hh:mm).
from-boot *seconds*	Displays event trace messages starting from a specified number of seconds after booting (uptime). To display the uptime, in seconds, enter the **showmonitorevent-trace**_component_**from-boot?** command.
latest	Displays only the event trace messages since the last **showmonitorevent-trace** command was entered.
parameters	Displays the trace parameters. The only parameter displayed is the size (number of trace messages) of the trace file.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(18)S	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S. The **showmonitorevent-tracecef** command replaced the **showcefevents**and **showipcefevents** commands.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
	The **spa** component keyword was added to support online insertion and removal (OIR) event messages for shared port adapters (SPAs).
	The **bfd** keyword was added for the *component* argument to display trace messages relating to the Bidirectional Forwarding Detection (BFD) feature.
12.4(4)T	Support for the **bfd** keyword was added for Cisco IOS Release 12.4(4)T.
12.0(31)S	Support for the **bfd** keyword was added for Cisco IOS Release 12.0(31)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.
12.4(9)T	The **cfd** keyword was added as an entry for the *component* argument to display trace messages relating to crypto fault detection.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use the **showmonitorevent-trace** command to display trace message information.

The trace function is not locked while information is being displayed to the console, which means that new trace messages can accumulate in memory. If entries accumulate faster than they can be displayed, some messages can be lost. If this happens, the **showmonitorevent-trace** command will generate a message

indicating that some messages might be lost; however, messages will continue to display on the console. If the number of lost messages is excessive, the **showmonitorevent-trace**command will stop displaying messages.

Use the **bfd** keyword for the *component* argument to display trace messages relating to the BFD feature.

Use the **cfd** keyword for the *component* argument to display trace messages relating to the crypto fault detection feature. This keyword displays the contents of the error trace buffers in an encryption data path.

Command Examples

Examples

The following is sample output from the **showmonitorevent-trace***component* command for the interprocess communication (IPC) component. Notice that each trace message is numbered and is followed by a time stamp (derived from the device uptime). Following the time stamp is the component-specific message data.

```
Router# show monitor event-trace ipc

3667:  6840.016:Message type:3 Data=0123456789
3668:  6840.016:Message type:4 Data=0123456789
3669:  6841.016:Message type:5 Data=0123456789
3670:  6841.016:Message type:6 Data=0123456
```

Examples

Use the **showmonitorevent-tracebfdall**command to display logged messages for important BFD events in the recent past. The following trace messages show BFD session state changes:

```
Router# show monitor event-trace bfd all
    3d03h: EVENT: Session [172.16.10.2,172.16.10.1,Fa6/0,1], event Session
          create, state Unknown -> Fail
    3d03h: EVENT: Session [172.16.10.2,172.16.10.1,Fa6/0,1], state Fail -> Down
           (from LC)
    3d03h: EVENT: Session [172.16.10.2,172.16.10.1,Fa6/0,1], state Down -> Init
           (from LC)
    3d03h: EVENT: Session [172.16.10.2,172.16.10.1,Fa6/0,1], state Init -> Up
          (from LC)
    3d07h: EVENT: Session [172.16.10.2,172.16.10.1,Fa6/0,2], event Session
          create, state Unknown -> Fail
    3d07h: EVENT: Session [172.16.10.2,172.16.10.1,Fa6/0,2], state Fail -> Down
           (from LC)
    3d07h: EVENT: Session [172.16.10.2,172.16.10.1,Fa6/0,2], state Down -> Up
          (from LC)
```

To display trace information for all components configured for event tracing on the networking device, enter the **showmonitorevent-traceall-traces** command. In this example, separate output is provided for each event, and message numbers are interleaved between the events.

```
Router# show monitor event-trace all-traces

Test1 event trace:
3667: 6840.016:Message type:3 Data=0123456789
3669: 6841.016:Message type:4 Data=0123456789
3671: 6842.016:Message type:5 Data=0123456789
3673: 6843.016:Message type:6 Data=0123456789
Test2 event trace:
3668: 6840.016:Message type:3 Data=0123456789
3670: 6841.016:Message type:4 Data=0123456789
3672: 6842.016:Message type:5 Data=0123456789
3674: 6843.016:Message type:6 Data=0123456789
```

Examples

The following is sample output from the **showmonitorevent-trace***component***latest** command for the **spa** component:

```
Router# show monitor event-trace spa latest
00:01:15.364: subslot 2/3: 4xOC3 POS SPA, TSM Event:inserted  New state:wait_psm
_ready
     spa type 0x440
00:02:02.308: subslot 2/0: not present, TSM Event:empty  New state:remove
     spa type 0x0, fail code 0x0(none)
00:02:02.308: subslot 2/0: not present, TSM Event:remove_complete  New state:idle
00:02:02.308: subslot 2/1: not present, TSM Event:empty  New state:remove
     spa type 0x0, fail code 0x0(none)
00:02:02.308: subslot 2/1: not present, TSM Event:remove_complete  New state:idle
00:02:02.308: subslot 2/2: not present, TSM Event:empty  New state:remove
     spa type 0x0, fail code 0x0(none)
00:02:02.308: subslot 2/2: not present, TSM Event:remove_complete  New state:idle
00:02:02.312: subslot 2/3: not present(plugin 4xOC3 POS SPA), TSM Event:empty  New
state:remove
     spa type 0x0, fail code 0x0(none)
00:02:02.312: subslot 2/3: not present, TSM Event:remove_complete  New state:idle
```

Examples

If you select Cisco Express Forwarding as the component for which to display event messages, you can use the following additional arguments and keywords: **showmonitorevent-tracecef** [**events** | **interface**|**ipv6** | **ipv4**][**all**].

The following example shows the IPv6 or IPv4 events related to the Cisco Express Forwarding component. Each trace message is numbered and is followed by a time stamp (derived from the device uptime). Following the time stamp is the component-specific message data.

```
Router# show monitor event-trace cef ipv6 all
00:00:24.612:  [Default] *::*/*'00          New FIB table          [OK]
Router# show monitor event-trace cef ipv4 all
00:00:24.244:  [Default] 127.0.0.81/32'01     FIB insert          [OK]
```

In the following example, all event trace messages for the Cisco Express Forwarding component are displayed:

```
Router# show monitor event-trace cef events all
00:00:18.884: SubSys  fib_ios_chain init
00:00:18.884: Inst    unknown -> RP
00:00:24.584: SubSys  fib init
00:00:24.592: SubSys  fib_ios init
00:00:24.592: SubSys  fib_ios_if init
00:00:24.596: SubSys  ipv4fib init
00:00:24.608: SubSys  ipv4fib_ios init
00:00:24.612: SubSys  ipv6fib_ios init
00:00:24.620: Flag    IPv4 CEF enabled set to yes
00:00:24.620: Flag    0x7BF6B62C set to yes
00:00:24.620: Flag    IPv4 CEF switching enabled set to yes
00:00:24.624: GState  CEF enabled
00:00:24.628: SubSys  ipv4fib_les init
00:00:24.628: SubSys  ipv4fib_pas init
00:00:24.632: SubSys  ipv4fib_util init
00:00:25.304: Process Background created
00:00:25.304: Flag    IPv4 CEF running set to yes
00:00:25.304: Process Background event loop enter
00:00:25.308: Flag    IPv4 CEF switching running set to yes
```

The following example shows Cisco Express Forwarding interface events:

```
Router# show monitor event-trace cef interface all
00:00:24.624: <empty>      (sw  4) Create   new
00:00:24.624: <empty>      (sw  4) SWIDBLnk FastEthernet0/0(4)
00:00:24.624: Fa0/0        (sw  4) NameSet
00:00:24.624: <empty>      (hw  1) Create   new
```

```
00:00:24.624: <empty>      (hw  1) HWIDBLnk FastEthernet0/0(1)
00:00:24.624: Fa0/0        (hw  1) NameSet
00:00:24.624: <empty>      (sw  3) Create   new
00:00:24.624: <empty>      (sw  3) SWIDBLnk FastEthernet0/1(3)
00:00:24.624: Fa0/1        (sw  3) NameSet
00:00:24.624: <empty>      (hw  2) Create   new
```

Examples

The following example shows the IPv4 events related to the Cisco Express Forwarding component. Each trace message is numbered and is followed by a time stamp (derived from the device uptime). Following the time stamp is the component-specific message data.

```
Router# show monitor event-trace cef ipv4 all
00:00:48.244: [Default] 127.0.0.81/32'01    FIB insert              [OK]
```

In the following example, all event trace message for the Cisco Express Forwarding component are displayed:

```
Router# show monitor event-trace cef events all
00:00:18.884: SubSys  fib_ios_chain init
00:00:18.884: Inst    unknown -> RP
00:00:24.584: SubSys  fib init
00:00:24.592: SubSys  fib_ios init
00:00:24.592: SubSys  fib_ios_if init
00:00:24.596: SubSys  ipv4fib init
00:00:24.608: SubSys  ipv4fib_ios init
00:00:24.620: Flag    IPv4 CEF enabled set to yes
00:00:24.620: Flag    0x7BF6B62C set to yes
00:00:24.620: Flag    IPv4 CEF switching enabled set to yes
00:00:24.624: GState  CEF enabled
00:00:24.628: SubSys  ipv4fib_les init
00:00:24.628: SubSys  ipv4fib_pas init
00:00:24.632: SubSys  ipv4fib_util init
00:00:25.304: Process Background created
00:00:25.304: Flag    IPv4 CEF running set to yes
00:00:25.304: Process Background event loop enter
00:00:25.308: Flag    IPv4 CEF switching running set to yes
```

The following examples show Cisco Express Forwarding interface events:

```
Router# show monitor event-trace cef interface all

00:00:24.624: <empty>      (sw  4) Create   new
00:00:24.624: <empty>      (sw  4) SWIDBLnk FastEthernet1/0/0(4)
00:00:24.624: Fa0/0        (sw  4) NameSet
00:00:24.624: <empty>      (hw  1) Create   new
00:00:24.624: <empty>      (hw  1) HWIDBLnk FastEthernet1/0/0(1)
00:00:24.624: Fa0/0        (hw  1) NameSet
00:00:24.624: <empty>      (sw  3) Create   new
00:00:24.624: <empty>      (sw  3) SWIDBLnk FastEthernet1/1/0(3)
00:00:24.624: Fa0/1        (sw  3) NameSet
00:00:24.624: <empty>      (hw  2) Create   new
```

Examples

To troubleshoot errors in an encryption datapath, enter the **showmonitorevent-tracecfdallcommand.Inthisexample,eventsareshownseparately,eachbeginningwithatimestamp,followedbydatafromtheerrortracebuffer.CiscoTechnicalAssistanceCenter(TAC)engineerscanusethisinformationtodiagnosethecauseoftheerrors.**

Note   If no packets have been dropped, this command does not display any output.

```
Router# show monitor event-trace cfd all
00:00:42.452: 450000B4 00060000 FF33B306 02020203 02020204 32040000 F672999C
             00000001 7A7690C2 A0A4F8BC E732985C D6FFDCC8 00000001 C0902BD0
             A99127AE 8EAA22D4
00:00:44.452: 450000B4 00070000 FF33B305 02020203 02020204 32040000 F672999C
             00000002 93C01218 2325B697 3C384CF1 D6FFDCC8 00000002 BFA13E8A
             D21053ED 0F62AB0E
00:00:46.452: 450000B4 00080000 FF33B304 02020203 02020204 32040000 F672999C
             00000003 7D2E11B7 A0BA4110 CC62F91E D6FFDCC8 00000003 7236B930
             3240CA8C 9EBB44FF
00:00:48.452: 450000B4 00090000 FF33B303 02020203 02020204 32040000 F672999C
             00000004 FB6C80D9 1AADF938 CDE57ABA D6FFDCC8 00000004 E10D8028
             6BBD748F 87F5E253
00:00:50.452: 450000B4 000A0000 FF33B302 02020203 02020204 32040000 F672999C
             00000005 697C8D9D 35A8799A 2A67E97B D6FFDCC8 00000005 BC21669D
             98B29FFF F32670F6
00:00:52.452: 450000B4 000B0000 FF33B301 02020203 02020204 32040000 F672999C
             00000006 CA18CBC4 0F387FE0 9095C27C D6FFDCC8 00000006 87A54811
             AE3A0517 F8AC4E64
```

Related Commands

Command	Description
monitor event-trace (EXEC)	Controls event trace functions for a specified Cisco IOS software subsystem component.
monitor event-trace (global)	Configures event tracing for a specified Cisco IOS software subsystem component.
monitor event-trace dump-traces	Saves trace messages for all event traces currently enabled on the networking device.

show platform hardware qfp active feature cef-mpls prefix ip

To display the interface name along with the interface descriptor block (IDB) information, use the **showplatformhardwareqfpactivefeaturecef-mplsprefixip** command in privileged EXEC.

> **show platform hardware qfp active feature cef-mpls prefix ip** {*ipv4 prefix* | [**vrf** [*id*]] [**exact**] [**brief**]}

Syntax Description

ipv4 prefix	IPv4 address and mask.
vrf	(Optional) Displays information about VPN Routing and Forwarding (VRF).
id	(Optional) Information about the particular VRF instance. The range is from 0 to 4294967295. If no VRF ID is specified, information about the global VRF, which is the prefix in global routing table, is displayed.
exact	(Optional) Find and displays the exact match of the IPV4 prefix.
brief	(Optional) Displays a summary of prefix information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)XNB	This command was introduced on the Cisco ASR 1000 Series Routers.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS Release XE 3.4S. Support for IP Fast Reroute (IP FRR) was added.

Command Examples

The following is sample output from the **showplatformhardwareqfpactivefeaturecef-mplsprefixip** command:

```
Router# show platform hardware qfp active feature cef-mpls prefix ip 0.0.0.0/1 vrf
Gtrie Node Type: Leaf Node
HW Content: : 00002000 00000000 897daf40 895db490
  QPPB QoS Precedence valid: 0
  QoS Precedence: 0
```

```
   QPPB QoS Group valid: 0
   QoS Group: 0
   BGPPA Traffic Index valid: 0
   BGPPA Traffic Index: 0
   TBLF refcount: 2
   TBLF application lf handle: 0
   Prefix Length: 32
   Prefix: 64 00 00 01
=== uRPF path list ===
   Loose Flag: : 1
   Path list pointer: : 0x8b8414a0
   Number of interfaces: : 1
   Interfaces: : 1017
   Interface Name(s): GigabitEthernet0/3/1
=== OCE ===
OCE Type: Adjacency, Number of children: 0
Adj Type: : IPV4 Adjacency
Encap Len: : 14
L3 MTU: : 1500
Adj Flags: : 0
Fixup Flags: : 0
Output UIDB: : 65522
Interface Name: GigabitEthernet0/3/1
Encap: : 00 14 f1 74 9c 1a 00 1a 30 44 3a 31 08 00
Next Hop Address: : 64000001 00000000 00000000 00000000
Oce Chain: : 0
```

The following example shows the output with the names of each interface when there are multiple interfaces in the unicast reverse path forwarding (uRPF) path list:

Router# show platform hardware qfp active feature cef-mpls prefix ip 0.0.0.0/2 vrf

```
Gtrie Node Type: Leaf Node
HW Content: : 00001800 00000000 897dae00 895d8df0
   QPPB QoS Precedence valid: 0
   QoS Precedence: 0
   QPPB QoS Group valid: 0
   QoS Group: 0
   BGPPA Traffic Index valid: 0
   BGPPA Traffic Index: 0
   TBLF refcount: 2
   TBLF application lf handle: 0
   Prefix Length: 24
   Prefix: 4d 4d 4d
=== uRPF path list ===
   Loose Flag: : 1
   Path list pointer: : 0x8b8414a0
   Number of interfaces: : 2
   Interfaces: : 1019, 1017
   Interface Name(s): : GigabitEthernet0/0/4, GigabitEthernet0/3/1
```

show platform hardware qfp active feature cef-mpls prefix ipv6

To display the interface name, along with the interface descriptor block (IDB) information for IPv6 addressing, use the **show platform hardware qfp active feature cef-mpls prefix ipv6** command in privileged EXEC mode.

> **show platform hardware qfp active feature cef-mpls prefix ipv6** {*ipv6 prefix* | [**vrf** [*id*]] [**exact**] [**brief**]}

Syntax Description

ipv6-prefix	IPv6 address and prefix. The IPv6 prefix is in the range from 0 to 128.
vrf *id*	(Optional) Displays the particular VPN Routing and Forwarding (VRF) instance. The VRF ID is in the range from 0 to 4294967295. If no VRF ID is specified, information about the global VRF (prefix in global routing table) is displayed.
exact	(Optional) Finds and displays the exact match of the IPv6 prefix.
brief	(Optional) Displays a summary of prefix information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)XNC	This command was introduced on the Cisco ASR 1000 Series Routers.
Cisco IOS XE Release 3.4S	This command was intergrated into Cisco IOS XE Release 3.4S.

Command Examples

The following is sample output from the **show platform hardware qfp active feature cef-mpls prefix ipv6** command:

```
Router# show platform hardware qfp active feature cef-mpls prefix ipv6 2001:DB8::/64

=== Gtrie Node ===

Gtrie Node Type: Tree Node
```

```
HW Content: : 89d000cd 00000004 60000000 00000000
Gtrie Tree Node Type:: Search Trie Node
=== Gtrie Search Node ===
  TN type 0, TN scan use 0, TN stride 6
  TN inode exists 1, TN skip 0
  TN zero perf real len: 0
  TN par bl offset: 0
  TN par bl len: 0
TBM Tree Array
  TA NNodes 2, TA INode Exists 1, TN TNRefs 0x11608698
TBM Tree Node Bitmap
Search Node Bitmap: 60 00 00 00 00 00 00 00
=== Gtrie Node ===

Gtrie Node Type: Leaf Node
HW Content: : 00004000 00000000 89995400 895c9420
  QPPB QoS Precedence valid: 0
  QoS Precedence: 0
  QPPB QoS Group valid: 0
  QoS Group: 0
  BGPPA Traffic Index valid: 0
  BGPPA Traffic Index: 0
  TBLF refcount: 2
  TBLF application lf handle: 0
  CTS src_sgt: 0
  CTS dst_sgt: 0
  Prefix Length: 64
  Prefix: cc 1e 00 00 00 00 00 00
  Lisp local eid: 0
  Lisp remote eid: 0
  Lisp locator status bits: 0
=== uRPF path list ===
  Loose Flag: : 1
  Path list pointer: : 0x895c9670
  Number of interfaces: : 1
  Interfaces: : 1015
  Interface Name(s): : GigabitEthernet0/2/0
=== OCE ===

OCE Type: Adjacency, Number of children: 0
Adj Type: : Glean Adjacency
Encap Len: : 0
L3 MTU: : 0
Adj Flags: : 0
Fixup Flags: : 0
Interface Name:
Next Hop Address: : 00000000 00000000 00000000 00000000
Next HW OCE Ptr: : 00000000
```

show platform hardware qfp active feature cef-mpls prefix mpls

To display the interface name, along with the interface descriptor block (IDB) information, use the show platform hardware qfp active feature cef-mpls prefix mpls command in privileged EXEC mode.

show platform hardware qfp active feature cef-mpls prefix mpls *label* [**vrf** [*id*]] [**exact**] [**brief**]

Syntax Description

label	Multiprotocol Label Switching (MPLS) label. The range is from 0 to 1048575.
vrf	(Optional) Displays information about VPN Routing and Forwarding (VRF).
id	(Optional) Information about the particular VRF instance. The range is from 0 to 4294967295. If no VRF ID is specified, information about the global VRF, which is the prefix in global routing table, is displayed.
exact	(Optional) Finds and displays the exact match of the prefix.
brief	(Optional) Displays a summary of prefix information.

Command Modes   Privileged EXEC (#)

Command History

Release	Modification
12.2(33)XNC	This command was introduced on the Cisco ASR 1000 Series Routers.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.

Command Examples   The following is sample output from the show platform hardware qfp active feature cef-mpls prefix mpls command:

```
Router# show platform hardware qfp active feature cef-mpls prefix mpls 0

=== Gtrie Node ===

Gtrie Node Type: Tree Node
HW Content: : 89b00cad 00000000 80000000 00000000
Gtrie Tree Node Type:: Search Trie Node
=== Gtrie Search Node ===
  TN type 0, TN scan use 0, TN stride 6
```

```
     TN inode exists 0, TN skip 0
     TN zero perf real len: 0
     TN par bl offset: 0
     TN par bl len: 0
  TBM Tree Array
     TA NNodes 1, TA INode Exists 0, TN TNRefs 0x116085e8
  TBM Tree Node Bitmap
  Search Node Bitmap: 80 00 00 00 00 00 00 00
  === Gtrie Node ===

  Gtrie Node Type: Tree Node
  HW Content: : 89b00cbd 00000000 80000000 00000000
  Gtrie Tree Node Type:: Search Trie Node
  === Gtrie Search Node ===
     TN type 0, TN scan use 0, TN stride 6
     TN inode exists 0, TN skip 0
     TN zero perf real len: 0
     TN par bl offset: 0
     TN par bl len: 0
  TBM Tree Array
     TA NNodes 1, TA INode Exists 0, TN TNRefs 0x116093d8
  TBM Tree Node Bitmap
  Search Node Bitmap: 80 00 00 00 00 00 00 00
  === Gtrie Node ===

  Gtrie Node Type: Leaf Node
  HW Content: : 0a000000 00000f00 00000000 895c97f0
     QPPB QoS Precedence valid: 0
     QoS Precedence: 0
     QPPB QoS Group valid: 0
     QoS Group: 0
     BGPPA Traffic Index valid: 0
     BGPPA Traffic Index: 0
     TBLF refcount: 2
     TBLF application lf handle: 0
     CTS src_sgt: 0
     CTS dst_sgt: 0
     Prefix Length: 20
     Prefix: 00 00 00
     Lisp local eid: 0
     Lisp remote eid: 0
     Lisp locator status bits: 0
  === OCE ===

  OCE Type: EOS OCE, Number of children: 2
     Next HW OCE Ptr: : 0x895c97d0, 0x895c97b0
  === OCE ===

  OCE Type: Label OCE, Number of children: 1
     Label flags: : 65
     Num Labels: : 1
     Num Bk Labels: : 0
     Out Labels: : 3
     Next HW OCE Ptr: : 0x895c9790
  === OCE ===

  OCE Type: Lookup OCE, Number of children: 0
     Lookup flags: : 1
     Table Type: : 0
     Lookup table ID: : 0
```

show route-map

To display static and dynamic route maps, use the **showroute-map** command in privileged EXEC mode.

show route-map [*map-name* | **dynamic** [*dynamic-map-name* | **application** [*application-name*]] | **all**] [**detailed**]

Syntax Description

map-name	(Optional) Name of a specific route map.
dynamic	(Optional) Displays dynamic route map information.
dynamic-map-name	(Optional) Name of a specific dynamic route map.
application	(Optional) Displays dynamic route maps based on applications.
application-name	(Optional) Name of a specific application.
all	(Optional) Displays all static and dynamic route maps.
detailed	(Optional) Displays the details of the access control lists (ACLs) that have been used in the **match** clauses for dynamic route maps.

Command Modes   Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S, and support for continue clauses was integrated into the command output.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(27)SBA	The output was enhanced to display dynamically assigned route maps to VRF tables.
12.2(15)T	An additional counter collect policy routing statistic was integrated into Cisco IOS Release 12.2(15)T.

Release	Modification
12.3(2)T	Support for continue clauses was integrated into Cisco IOS Release 12.3(2)T.
12.2(17b)SXA	This command was integrated into Cisco IOS Release 12.2(17b)SXA.
12.3(7)T	The **dynamic**, **application**, and **all** keywords were added.
12.0(28)S	The support for recursive **next-hop** clause was added.
12.3(14)T	The support for recursive **next-hop** clause was integrated into Cisco IOS Release 12.3(14)T. Support for the map display extension functionality was added. The **detailed** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
Cisco IOS XE Release 2.2	In Cisco IOS XE Release 2.2 this command was introduced on the Cisco ASR 1000 Series Routers.
15.0(1)M	This command was modified. The **detailed** keyword was removed.
12.2(33)SXI4	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SXI4.

Usage Guidelines

You can view static and dynamic route maps with the **showroute-map** command. For Cisco IOS Release 12.3(14)T and later 12.4 and 12.4T releases, you can display the ACL-specific information that pertains to the route map in the same display without having to execute a **showroute-map**command to display each ACL that is associated with the route map.

Redistribution

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

The **matchroute-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 **routemaps** 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.

Command Examples

The **showroute-map** command will display configured route-maps, match, set, and continue clauses. The output will vary depending on which keywords are included with the command, and which software image is running in your router, as shown in the following examples:

Examples

The following is sample output from the show route-map command:

```
Router# show route-map
route-map ROUTE-MAP-NAME, permit, sequence 10
  Match clauses:
    ip address (access-lists): 1
    metric 10
  Continue: sequence 40
  Set clauses:
    as-path prepend 10
  Policy routing matches: 0 packets, 0 bytes
route-map ROUTE-MAP-NAME, permit, sequence 20
  Match clauses:
    ip address (access-lists): 2
    metric 20
  Set clauses:
    as-path prepend 10 10
  Policy routing matches: 0 packets, 0 bytes
route-map ROUTE-MAP-NAME, permit, sequence 30
  Match clauses:
  Continue: to next entry 40
  Set clauses:
    as-path prepend 10 10 10
  Policy routing matches: 0 packets, 0 bytes
route-map ROUTE-MAP-NAME, deny, sequence 40
  Match clauses:
    community (community-list filter): 20:2
  Set clauses:
    local-preference 100
  Policy routing matches: 0 packets, 0 bytes
route-map LOCAL-POLICY-MAP, permit, sequence 10
  Match clauses:
  Set clauses:
    community 655370
  Policy routing matches: 0 packets, 0 bytes
```

The following example shows Multiprotocol Label Switching (MPLS)-related route map information:

```
Router# show route-map
route-map OUT, permit, sequence 10
Match clauses:
  ip address (access-lists): 1
Set clauses:
  mpls label
Policy routing matches: 0 packets, 0 bytes

route-map IN, permit, sequence 10
Match clauses:
  ip address (access-lists): 2
```

```
  mpls label
Set clauses:
Policy routing matches: 0 packets, 0 bytes
```

The table below describes the significant fields shown in the display.

Table 26   show route-map Field Descriptions

Field	Description
route-map ROUTE-MAP-NAME	Name of the route map.
permit	Indicates that the route is redistributed as controlled by the set actions.
sequence	Number that indicates the position a new route map is to have in the list of route maps already configured with the same name.
Match clauses: tag	Match criteria--Conditions under which redistribution is allowed for the current route map.
Continue:	Continue clause--Shows the configuration of a continue clause and the route-map entry sequence number that the continue clause will go to.
Set clauses: metric	Set actions--The particular redistribution actions to perform if the criteria enforced by the **match** commands are met.
Policy routing matches:	Number of packets and bytes that have been filtered by policy routing.

Examples

The following is sample output from the show route-map command when entered with the dynamic keyword:

```
Router# show route-map dynamic
route-map AAA-02/06/04-14:01:26.619-1-AppSpec, permit, sequence 0, identifier 1137954548
  Match clauses:
    ip address (access-lists): PBR#1 PBR#2
  Set clauses:
  Policy routing matches: 0 packets, 0 bytes
route-map AAA-02/06/04-14:01:26.619-1-AppSpec, permit, sequence 1, identifier 1137956424
  Match clauses:
    ip address (access-lists): PBR#3 PBR#4
  Set clauses:
  Policy routing matches: 0 packets, 0 bytes
route-map AAA-02/06/04-14:01:26.619-1-AppSpec, permit, sequence 2, identifier 1124436704
  Match clauses:
    ip address (access-lists): PBR#5 PBR#6
    length 10 100
  Set clauses:
    ip next-hop 172.16.1.1
    ip gateway 172.16.1.1
  Policy routing matches: 0 packets, 0 bytes
Current active dynamic routemaps = 1
```

The following is sample output from the show route-map command when entered with the dynamic and **application** keywords:

```
Router# show route-map dynamic application
Application - AAA
  Number of active routemaps = 1
```

When you specify an application name, only dynamic routes for that application are shown. The following is sample output from the show route-map command when entered with the dynamic and **application** keywords and the AAA application name:

```
Router# show route-map dynamic application AAA
AAA
  Number of active rmaps = 2
AAA-02/06/04-14:01:26.619-1-AppSpec
AAA-02/06/04-14:34:09.735-2-AppSpec
Router# show route-map dynamic AAA-02/06/04-14:34:09.735-2-AppSpec
route-map AAA-02/06/04-14:34:09.735-2-AppSpec, permit, sequence 0, identifier 1128046100
  Match clauses:
    ip address (access-lists): PBR#7 PBR#8
  Set clauses:
  Policy routing matches: 0 packets, 0 bytes
route-map AAA-02/06/04-14:34:09.735-2-AppSpec, permit, sequence 1, identifier 1141277624
  Match clauses:
    ip address (access-lists): PBR#9 PBR#10
  Set clauses:
  Policy routing matches: 0 packets, 0 bytes
route-map AAA-02/06/04-14:34:09.735-2-AppSpec, permit, sequence 2, identifier 1141279420
  Match clauses:
    ip address (access-lists): PBR#11 PBR#12
    length 10 100
  Set clauses:
    ip next-hop 172.16.1.12
    ip gateway 172.16.1.12
  Policy routing matches: 0 packets, 0 bytes
Current active dynamic routemaps = 2
```

Examples

The following is sample output from the show route-map command with the **dynamic** and **detailed** keywords entered:

```
Router# show route-map dynamic detailed
route-map AAA-01/20/04-22:03:10.799-1-AppSpec, permit, sequence 1, identifier 29675368
Match clauses:
ip address (access-lists):
Extended IP access list PBR#3
1 permit icmp 0.0.16.12 1.204.167.240 10.1.1.0 0.0.0.255 syn dscp af12 log-input
fragments
Extended IP access list PBR#4
1 permit icmp 0.0.16.12 1.204.167.240 10.1.1.0 0.0.0.255 syn dscp af12 log-input
fragments
Set clauses:
ip next-hop 172.16.1.14
ip gateway 172.16.1.14
Policy routing matches: 0 packets, 0 bytes
```

Examples

The following is sample output from the **showroute-map** command when a specified VRF is configured for VRF autoclassification:

```
Router# show route-map dynamic
route-map None-06/01/04-21:14:21.407-1-IP VRF, permit, sequence 0
identifier 1675771000
 Match clauses:
```

```
 Set clauses: vrf red
 Policy routing matches: 0 packets, 0 bytes
Current active dynamic routemaps = 1
```

Related Commands

Command	Description
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
match interface (IP)	Distributes any routes that have their next hop out one of the interfaces specified.
match ip next-hop	Redistributes any routes that have a next hop router address passed by one of the access lists specified.
match tag	Redistributes routes in the routing table that match the specified tags.

traffic-share min

To c onfigure traffic to use minimum-cost routes, when there are multiple routes that have different-cost routes to the same destination network, use the**traffic-sharemin**command in router address family topology or router configuration mode. To disable this function, use the **no** form of this command.

traffic-share min commandtraffic-share min across-interfaces

no traffic-share min across-interfaces

Syntax Description

across-interfaces	Configures multi-interface load splitting on several interfaces with equal-cost paths.

Command Default

Traffic is configured to use minimum-cost paths.

Command Modes

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

Command History

Release	Modification
10.0	This command was introduced.
11.0(3)	This command became protocol independent when the **across-interfaces**keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was made available in router address family topology configuration mode.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **traffic-sharemin** command causes the Cisco IOS software to divide traffic only among the routes with the best metric. Other routes will remain in the routing table, but will receive no traffic. Configuring this command with the **across-interfaces** keyword allows you to configure multi-interface load splitting on different interfaces with equal-cost paths.

Release 12.2(33)SRB

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

Command Examples

In the following example, multi-interface load splitting is configured on different interfaces with equal-cost paths:

```
router ospf 5
 traffic-share min across-interfaces
```

VCCV

To configure the pseudowire Virtual Circuit Connection Verification (VCCV) control channel (CC) type for Multiprotocol Label Switching (MPLS) pseudowires, use the **vccv** command in pseudowire class configuration mode. To disable a pseudowire VCCV CC type, use the **no** form of this command.

vccv {**control-word** | **router-alert** | **ttl**}

no vccv {**control-word** | **router-alert** | **ttl**}

Syntax Description

control-word	Specifies the control channel (CC) Type 1: control word.
router-alert	Specifies the CC Type 2: MPLS router alert label.
ttl	Specifies the CC Type 3: MPLS pseudowire label with Time to Live (TTL).

Command Default   The pseudowire VCCV CC type is set to Type 1 (control word).

Command Modes   Pseudowire-class configuration (config-pw-class)

Command History

Release	Modification
15.0(1)S	This command was introduced.

Usage Guidelines   When an initiating provider edge (PE) device sends a setup request message to a remote PE device, the message includes VCCV capability information. This capability information is a combination of the CC type and the control verification (CV) type. You use the **vccv** command to configure the CC type capabilities of the MPLS pseudowire.

If the CV type for the MPLS pseudowire is set to a type that does not use IP/User Datagram Protocol (UDP) headers, then you must set the CC type to the CC Type 1: control word.

Command Examples   The following example shows how to configure the MPLS pseudowire class to use CC Type 1:

```
Router(config)# pseudowire-class bfdclass
Router(config-pw-class)# encapsulation mpls
Router(config-pw-class)# protocol none
Router(config-pw-class)# vccv control-word
```

Related Commands

Command	Description
bfd-template	Creates a BFD template and enters BFD configuration mode.
pseudowire-class	Specifies the name of the pseudowire class and enters pseudowire class configuration mode.
vccv bfd template	Enables VCCV BFD for a pseudowire class.
vccv bfd status signaling	Enables status signaling for BFD VCCV.

vccv bfd status signaling

To enable status signaling for Bidirectional Forwarding Detection (BFD) Virtual Circuit Connection Verification (VCCV), use the **vccvbfdstatussignaling**command in pseudowire class configuration mode. To disable status signaling, use the **no** form of this command.

vccv bfd status signaling

no vccv bfd status signaling

Syntax Description   This command has no arguments or keywords.

Command Default   VCCV BFD status signaling is disabled.

Command Modes   Pseudowire-class configuration (config-pw-class)

Command History

Release	Modification
15.0(1)S	This command was introduced.

Usage Guidelines   Use this command to allow BFD to provide status signaling functionality that indicates the fault status of an attachment circuit (AC).

Command Examples   The following example shows how to enable VCCV BFD status signaling for a Multiprotocol Label Switching (MPLS) pseudowire class:

```
Router(config)# pseudowire-class bfdclass
Router(config-pw-class)# encapsulation mpls
Router(config-pw-class)# protocol none
Router(config-pw-class)# vccv control-word
Router(config-pw-class)# vccv bfd template bfdtemplate raw-bfd
Router(config-pw-class)# vccv bfd status signaling
```

Related Commands

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

Command	Description
pseudowire-class	Specifies the name of the pseudowire class and enters pseudowire class configuration mode.
vccv	Configures the pseudowire VCCV CC type for MPLS pseudowires.
vccv bfd template	Enables VCCV BFD for a pseudowire class.

vccv bfd template

To enable Virtual Circuit Connection Verification (VCCV) Bidirectional Forwarding Detection (BFD) for a pseudowire class, use the **vccvbfdtemplate** command in pseudowire class configuration mode. To disable VCCV BFD, use the **no** form of this command.

vccv bfd template *name* [**udp** | **raw-bfd**]

no vccv bfd template *name* [**udp** | **raw-bfd**]

Syntax Description

name	The name of the BFD template to use.
udp	(Optional) Enables support for BFD with IP/User Datagram Protocol (UDP) header encapsulation.
raw-bfd	(Optional) Enables support for BFD without IP/UDP header encapsulation.

Command Default

VCCV BFD is not enabled for the pseudowire class.

Command Modes

Pseudowire-class configuration (config-pw-class)

Command History

Release	Modification
15.0(1)S	This command was introduced.

Usage Guidelines

The BFD template specified by the*name* argument is created using the **bfd-template**command, and contains settings for the BFD interval values.

VCCV defines two types encapsulation for VCCV messages to differentiate them from data packets: BFD with IP/UDP headers and BFD without IP/UDP headers.

Support for BFD without IP/UDP headers can be enabled only for pseudowires that use a control word, or a Layer 2 Specific Sublayer (L2SS) that can take the pseudowire associated Channel Header Control Word format.

If the VCCV carries raw BFD, the control word or the L2SS Channel Type must be set to BFD without IP/UDP headers. BFD without IP/UDP headers allows the system to identify the BFD packet when demultiplexing the control channel.

Command Examples   The following example shows how to enable the BFD template without support for IP/UDP header encapsulation:

```
Router(config)# pseudowire-class bfdclass
Router(config-pw-class)# encapsulation mpls
Router(config-pw-class)# protocol none
Router(config-pw-class)# vccv control-word
Router(config-pw-class)# vccv bfd template bfdtemplate raw-bfd
Router(config-pw-class)# vccv bfd status signaling
```