



## **Cisco IOS IP Routing: Protocol-Independent Command Reference**

### **Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2021 Cisco Systems, Inc. All rights reserved.



## CONTENTS

---

### CHAPTER 1

### IP Routing Protocol-Independent Commands: A through R 1

accept-ao-mismatch	3
accept-lifetime	4
authentication (BFD)	7
bfd	9
bfd all-interfaces	12
bfd check-ctrl-plane-failure	15
bfd echo	16
bfd interface	18
bfd map	20
bfd slow-timers	22
bfd template	24
bfd-template	25
cryptographic-algorithm	27
dampening	28
distance (IP)	30
distribute-list in (IP)	34
distribute-list out (IP)	39
fast-reroute load-sharing disable	42
fast-reroute per-prefix	43
fast-reroute tie-break	45
echo	47
include-tcp-options	49
interval (BFD)	50
ip default-network	52
ip gdp	54

ip local policy route-map	55
ip policy route-map	57
ip route	59
ip route profile	65
ip route static adjust-time	67
ip route static bfd	68
ip route static install-routes-recurse-via-next-hop	71
ip routing	73
ip routing protocol purge interface	74
ipv6 local policy route-map	75
ipv6 policy route-map	77
ipv6 route static bfd	79
isdn supp-service callRerouteing	81
ipv6 route static resolve default	82
key	83
key chain	86
key-string (authentication)	89
match interface (IP)	91
match ip address	93
match ip next-hop	97
match ip redistribution-source	99
match ip route-source	102
match ipv6 address	105
match length	108
match metric (IP)	111
match route-type (IP)	114
match tag	116
match tag list	118
match track	119
maximum-paths	120
monitor peer bfd	121
named-ordering-route-map enable	123
nsf	124
passive-interface	127

platform bfd allow-svi 129  
 platform bfd enable-offload 130  
 platform cloudsec padding-fixup 131  
 recv-id 133  
 redistribute (IP) 134  
 route-map 145  
 route-tag list 150  
 route-tag notation 151  
 routing dynamic 153

---

**CHAPTER 2**
**IP Routing Protocol-Independent Commands: S through T 155**

send-lifetime 157  
 send-id 160  
 set automatic-tag 162  
 set default interface 164  
 set interface 167  
 set ip default next-hop 170  
 set ip default next-hop verify-availability 172  
 set ip global 173  
 set ip next-hop 175  
 set ip next-hop verify-availability 178  
 set ip vrf 182  
 set ipv6 default next-hop 184  
 set ipv6 next-hop (PBR) 187  
 set ipv6 precedence 189  
 set level (IP) 191  
 set local-preference 193  
 set metric (BGP-OSPF-RIP) 195  
 set metric-type 197  
 set next-hop 199  
 set tag (IP) 201  
 set vrf next-hop verify-availability 203  
 show bfd drops 206  
 show bfd neighbors 208

show bfd summary	219
show dampening interface	221
show fm ipv6 pbr all	223
show fm ipv6 pbr interface	224
show interface dampening	225
show ip cef platform	227
show ip cache policy	229
show ip local policy	231
show ip policy	233
show ip protocols	235
show ip route	242
show ip route loops	255
show ip route profile	256
show ip route summary	258
show ip route supernets-only	260
show ip route tag	261
show ip route track-table	264
show ip static route	265
show ip static route bfd	266
show ip route vrf	268
show ipv6 policy	275
show ipv6 route	276
show ipv6 route shortcut	281
show ipv6 route summary	283
show ipv6 route tag	285
show ipv6 route vrf	287
show isis fast-reroute	290
show key chain	292
show monitor event-trace	293
show platform hardware qfp active feature cef-mpls prefix ip	299
show platform hardware qfp active feature cef-mpls prefix ipv6	301
show platform hardware qfp active feature cef-mpls prefix mpls	303
show platform software ip fp active cloudsec	305
show platform software ip rp active cloudsec	306

show route-map	307
show route-tag list	312
traffic-share min	314
vccv	315
vccv bfd status signaling	317
vccv bfd template	319







# IP Routing Protocol-Independent Commands: A through R

---

- [accept-ao-mismatch](#), on page 3
- [accept-lifetime](#), on page 4
- [authentication \(BFD\)](#), on page 7
- [bfd](#), on page 9
- [bfd all-interfaces](#), on page 12
- [bfd check-ctrl-plane-failure](#), on page 15
- [bfd echo](#), on page 16
- [bfd interface](#), on page 18
- [bfd map](#), on page 20
- [bfd slow-timers](#), on page 22
- [bfd template](#), on page 24
- [bfd-template](#), on page 25
- [cryptographic-algorithm](#), on page 27
- [dampening](#), on page 28
- [distance \(IP\)](#), on page 30
- [distribute-list in \(IP\)](#), on page 34
- [distribute-list out \(IP\)](#), on page 39
- [fast-reroute load-sharing disable](#), on page 42
- [fast-reroute per-prefix](#), on page 43
- [fast-reroute tie-break](#), on page 45
- [echo](#), on page 47
- [include-tcp-options](#), on page 49
- [interval \(BFD\)](#), on page 50
- [ip default-network](#), on page 52
- [ip gdp](#), on page 54
- [ip local policy route-map](#), on page 55
- [ip policy route-map](#), on page 57
- [ip route](#), on page 59
- [ip route profile](#), on page 65
- [ip route static adjust-time](#), on page 67
- [ip route static bfd](#), on page 68

- [ip route static install-routes-recurse-via-next-hop](#), on page 71
- [ip routing](#), on page 73
- [ip routing protocol purge interface](#), on page 74
- [ipv6 local policy route-map](#), on page 75
- [ipv6 policy route-map](#), on page 77
- [ipv6 route static bfd](#), on page 79
- [isdn supp-service callRerouteing](#), on page 81
- [ipv6 route static resolve default](#), on page 82
- [key](#), on page 83
- [key chain](#), on page 86
- [key-string \(authentication\)](#), on page 89
- [match interface \(IP\)](#), on page 91
- [match ip address](#), on page 93
- [match ip next-hop](#), on page 97
- [match ip redistribution-source](#), on page 99
- [match ip route-source](#), on page 102
- [match ipv6 address](#), on page 105
- [match length](#), on page 108
- [match metric \(IP\)](#), on page 111
- [match route-type \(IP\)](#), on page 114
- [match tag](#), on page 116
- [match tag list](#), on page 118
- [match track](#), on page 119
- [maximum-paths](#), on page 120
- [monitor peer bfd](#), on page 121
- [named-ordering-route-map enable](#), on page 123
- [nsf](#), on page 124
- [passive-interface](#), on page 127
- [platform bfd allow-svi](#), on page 129
- [platform bfd enable-offload](#), on page 130
- [platform cloudsec padding-fixup](#), on page 131
- [recv-id](#), on page 133
- [redistribute \(IP\)](#), on page 134
- [route-map](#), on page 145
- [route-tag list](#), on page 150
- [route-tag notation](#), on page 151
- [routing dynamic](#), on page 153

# accept-ao-mismatch

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

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

## accept-ao-mismatch

### Command Default

By default this option is disabled.

### Command Modes

Key chain key configuration (config-keychain-key)

### Command History

Release	Modification
16.12.1	This command was introduced.

### Usage Guidelines

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

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

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

```
Router(config)# key chain kcl tcp
Router(config-keychain)# key 7890
Router(config-keychain-key)# send-id 215
Router(config-keychain-key)# rcv-id 215
Router(config-keychain-key)# key-string k1omn
Router(config-keychain-key)# accept-ao-mismatch
```

### Related Commands

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

## accept-lifetime

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

```
accept-lifetime start-time {infiniteend-time | duration seconds}
no accept-lifetime [start-time {infiniteend-time | duration seconds}]
```

Syntax Description	
<i>start-time</i>	Beginning time that the key specified by the <b>key</b> command is valid to be received. The syntax can be either of the following:  <i>hh</i> : <i>mm</i> : <i>ss</i> <i>Month</i> <i>date</i> <i>year</i> <i>hh</i> : <i>mm</i> : <i>ss</i> <i>date</i> <i>Month</i> <i>year</i> <ul style="list-style-type: none"> <li>• <i>hh</i> --hours</li> <li>• <i>mm</i> --minutes</li> <li>• <i>ss</i>-- s econds</li> <li>• <i>Month</i>-- first three letters of the month</li> <li>• <i>date</i>-- date (1-31)</li> <li>• <i>year</i>-- y ear (four digits)</li> </ul> <p>The default start time and the earliest acceptable date is January 1, 1993.</p>
<b>infinite</b>	Key is valid to be received from the <i>start-time</i> value on.
<i>end-time</i>	Key is valid to be received from the <i>start-time</i> value until the <i>end-time</i> value. The syntax is the same as that for the <i>start-time</i> value. The <i>end-time</i> value must be after the <i>start-time</i> value. The default end time is an infinite time period.
<b>duration</b> <i>seconds</i>	Length of time (in seconds) that the key is valid to be received. The range is from 1 to 2147483646.

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

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

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

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

### Usage Guidelines

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

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

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

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

### Examples

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

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

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

```
Router(config)# router
  eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# network 10.0.0.0
Router(config-router-af)# af-interface ethernet0/0
Router(config-router-af-interface)# authentication key-chain trees
Router(config-router-af-interface)# authentication mode md5
Router(config-router-af-interface)# exit
Router(config-router-af)# exit
```

```

Router(config-router)# exit
Router(config)# key chain chain1
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string key1
Router(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 14:00:00 Jan 25 1996 duration 3600
Router(config-keychain-key)# exit
Router(config-keychain)# key 2
Router(config-keychain-key)# key-string key2
Router(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 15:00:00 Jan 25 1996 duration 3600

```

**Related Commands**

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

## authentication (BFD)

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

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

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

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

**Command Modes** BFD configuration (config-bfd)

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

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

### Examples

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

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

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

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

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>bfd</b>	Sets the baseline BFD session parameters on an interface.
<b>bfd map</b>	Configures a BFD map that associates timers and authentication with multihop templates.
<b>bfd-template</b>	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		
<b>interval</b> <i>milliseconds</i>		Specifies the rate, in milliseconds, at which BFD control packets will be sent to BFD peers. The valid range for the <i>milliseconds</i> argument is from 50 to 999.
<b>min_rx</b> <i>milliseconds</i>		Specifies the rate, in milliseconds, at which BFD control packets will be expected to be received from BFD peers. The valid range for the <i>milliseconds</i> argument is from 50 to 999.
<b>multiplier</b> <i>multiplier-value</i>		Specifies the number of consecutive BFD control packets that must be missed from a BFD peer before BFD declares that the peer is unavailable and the Layer 3 BFD peer is informed of the failure. The valid range for the <i>multiplier-value</i> argument is from 3 to 50.

**Command Default** No baseline BFD session parameters are set.

**Command Modes** Interface configuration (config-if)

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

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

### Usage Guidelines

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

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

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



### Note

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

The **bfd interval** configuration is not removed when:

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

The **bfd interval** configuration is removed when:

- the subinterface on which it is configured is removed

## Examples

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

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

## Related Commands

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

## bfd all-interfaces

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

**bfd all-interfaces**

**no bfd all-interfaces**

### Syntax Description

This command has no arguments or keywords.

### Command Default

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

### Command Modes

Router configuration (config-router)

Address family interface configuration (config-router-af)

### Command History

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

### Usage Guidelines

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

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

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

## Examples

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

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

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

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

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

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

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

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

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

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

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

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

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>bfd</b>	Sets the baseline BFD session parameters on an interface.

# bfd check-ctrl-plane-failure

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

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

**Syntax Description** This command has no arguments or keywords.

**Command Default** BFD control plane failure checking is disabled.

**Command Modes** Router configuration (config-router)

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

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

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

## Examples

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

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

## Related Commands

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

# bfd echo

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

**bfd echo**  
**no bfd echo**

**Syntax Description** This command has no arguments or keywords.

**Command Default** BFD echo mode is enabled by default.

**Command Modes** Interface configuration (config-if)

## Command History

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

## Usage Guidelines

Echo mode is enabled by default. Entering the **no bfdecho** 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 **bfdintervalmilliseconds****min\_rxm****milliseconds** parameters, respectively.



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



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

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

### Echo Mode Without Asymmetry

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



**Examples**

The following example configures echo mode between BFD neighbors:

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

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

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

**Related Commands**

Command	Description
<b>bfd</b>	Sets the baseline BFD session parameters on the interface.
<b>ip redirects</b>	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.
<b>ip route-cache</b>	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	Field	Description
	<i>type</i>	Interface type for the interface to be enabled for BFD.
	<i>number</i>	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 <b>bfdinterface</b> command in named router configuration mode was replaced by the <b>bfd</b> 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 interface mode (af-interface mode).

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

### Examples

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

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

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

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

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

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

**Related Commands**

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

## bfd map

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

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

### Syntax Description

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

### Command Default

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

### Command Modes

Global configuration (config)

### Command History

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

### Usage Guidelines

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

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

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

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

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

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

## Examples

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

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

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

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

## Related Commands

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

<i>milliseconds</i>	(Optional) BFD slow timers value, in milliseconds. The range is from 1000 to 30000. The default is 1000.
---------------------	--

### Command Default

The BFD slow timer value is 1000 milliseconds.

### Command Modes

Global configuration (config)

### Command History

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

### Examples

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

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

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

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

**Related Commands**

Command	Description
<b>bfd echo</b>	Enables BFD echo mode.

# bfd template

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

```
bfd template template-name
no bfd template template-name
```

<b>Syntax Description</b>	<i>template-name</i>	Name of the BFD template.
---------------------------	----------------------	---------------------------

**Command Default** A BFD template is not bound to an interface.

**Command Modes** Interface configuration (config-if)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	15.2(4)S	This command was introduced.
	Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.

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

## Examples

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

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>bfd-template</b>	Creates a BFD template and enters BFD configuration mode.



# bfd-template

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

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

## Syntax Description

<b>single-hop</b>	Creates the single-hop BFD template.
<b>multi-hop</b>	Creates the multihop BFD template.
<i>template-name</i>	Template name.

## Command Default

A BFD template does not exist.

## Command Modes

Global configuration (config)

## Command History

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

## Usage Guidelines

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

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

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

## Examples

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

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

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

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

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

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

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

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

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

#### Related Commands

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

# cryptographic-algorithm

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

**cryptographic-algorithm** *algorithm*

<b>Syntax Description</b>	<p><i>algorithm</i></p> <p>Specify one of the following authentication algorithms:</p> <ul style="list-style-type: none"> <li>• <code>aes-128-cmac</code>- AES-128-CMAC algorithm</li> <li>• <code>hmac-sha-1</code>- HMAC-SHA-1 algorithm</li> <li>• <code>hmac-sha-256</code>- HMAC-SHA-256 algorithm</li> </ul>
---------------------------	--

**Command Default** No algorithm is specified.

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

<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>16.12.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	16.12.1	This command was introduced.
Release	Modification				
16.12.1	This command was introduced.				

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

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

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

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

<b>Related Commands</b>	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><b>key</b></td> <td>Identifies an authentication key on a key chain.</td> </tr> <tr> <td><b>key chain</b> <i>key-name</i> <b>tcp</b></td> <td>Defines a TCP-AO authentication key-chain needed to enable authentication for routing protocols.</td> </tr> <tr> <td><b>key-string</b> (authentication)</td> <td>Specifies the authentication string for a key.</td> </tr> <tr> <td><b>show key chain</b></td> <td>Displays authentication key information.</td> </tr> </tbody> </table>	Command	Description	<b>key</b>	Identifies an authentication key on a key chain.	<b>key chain</b> <i>key-name</i> <b>tcp</b>	Defines a TCP-AO authentication key-chain needed to enable authentication for routing protocols.	<b>key-string</b> (authentication)	Specifies the authentication string for a key.	<b>show key chain</b>	Displays authentication key information.
Command	Description										
<b>key</b>	Identifies an authentication key on a key chain.										
<b>key chain</b> <i>key-name</i> <b>tcp</b>	Defines a TCP-AO authentication key-chain needed to enable authentication for routing protocols.										
<b>key-string</b> (authentication)	Specifies the authentication string for a key.										
<b>show key chain</b>	Displays authentication key information.										

# dampening

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

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

## Syntax Description

<i>half-life-period</i>	(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.
<i>reuse-threshold</i>	(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.
<i>suppress-threshold</i>	(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.
<i>max-suppress-time</i>	(optional) Maximum time (in seconds) a route can be suppressed. The range is from 1 to 20000; the default is four times the <i>half-life-periodvalue</i> . If the <i>half-life-period</i> value is allowed to default, the maximum suppress time defaults to 20 seconds.
<i>restart-penalty</i>	(optional) Penalty to applied to the interface when it comes up for the first time after the router reloads. The configurable range is from 1 to 18000 penalties. The default is 2000 penalties. This argument is not required for any other configurations.

## Command Default

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

## Command Modes

Interface configuration (config-if)

## Command History

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

**Usage Guidelines**

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

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

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

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

**Examples**

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

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

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

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

**Related Commands**

Command	Description
<b>clear counters</b>	Clears the interface counters.
<b>show dampening interface</b>	Displays a summary of interface dampening.
<b>show interface dampening</b>	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**access-list-name*}]

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

### Syntax Description

<i>distance</i>	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.)
<i>ip-address</i>	IP address in four-part, dotted decimal notation. The IP address or the network address from where routes are learned.
<i>wildcard-mask</i>	Wildcard mask in four-part, dotted decimal notation. A bit set to 1 in the <i>wildcard-mask</i> argument instructs the software to ignore the corresponding bit in the address value.
<i>ip-standard-acl</i>	(Optional) Standard IP access list (ACL) number to be applied to incoming routing updates.
<i>access-list-name</i>	(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 <i>access-list-name</i> argument was added.
11.3	This command was modified. The <i>ip</i> keyword was removed.
12.0	This command was modified. The <i>ip-standard-acl</i> and <i>ip-extended-acl</i> arguments were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.0(1)M	This command was integrated into a release earlier than Cisco IOS Release 15.0(1)M.
15.2(4)S	This command was modified. The <i>ip-extended-acl</i> argument was removed.

**Usage Guidelines**

The table below lists default administrative distances.

**Table 1: Default Administrative Distances**

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

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

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



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

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

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

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

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

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



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

## Examples

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

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

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

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



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

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

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



```

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

```

**Related Commands**

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

## distribute-list in (IP)

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

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

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

### Syntax Description

<i>access-list-name</i>	IP access-list name. The <i>access-list-name</i> argument defines which networks are to be received and which are to be suppressed in routing updates. <ul style="list-style-type: none"> <li>The range is from 1 to 199.</li> </ul>
<i>access-list-number</i>	IP access-list number. The <i>access-list-number</i> argument defines which networks are to be received and which are to be suppressed in routing updates.
<b>gateway</b>	Filters incoming address updates based on a gateway.
<i>prefix-list-name</i>	IP prefix-list name. The <i>prefix-list-name</i> argument defines which routes from specified IP prefixes in the routing table are to be received and which are to be suppressed in routing updates.
<b>prefix</b>	Filters prefixes in address updates.
<i>interface-type</i>	(Optional) Type of interface. The <i>interface-type</i> argument defines the type of interface from which routing updates are to be received or suppressed.  The <i>interface-type</i> argument cannot be used in address family configuration mode.
<i>interface-number</i>	(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 <i>interface-type</i> and <i>interface-number</i> arguments are applied if you specify an access list, not a route map. The <i>interface-number</i> argument cannot be used in address family configuration mode.
<b>route-map</b>	Specifies the route map that defines which networks are to be installed in the routing table and which are to be filtered from the routing table.
<i>route-map-name</i>	Name of route-map. The <i>route-map-name</i> argument defines the networks from which routing updates are to be received or suppressed. This argument is supported by OSPF, EIGRP and IS-IS.

### Command Default

Networks received in updates are not filtered.

**Command Modes**

Router configuration (config-router)

Address family configuration (config-router-af)

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

**Command History**

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

**Usage Guidelines**

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

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

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

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

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

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

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

### Release 12.2(33)SRB

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

## Examples

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

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

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

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

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

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

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

```

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

```

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

```

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

```

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

```

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

```

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

```

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

```

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

```

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

```

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

```

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

```

**distribute-list in (IP)**

```
Device(config-router-af) # distribute-list prefix-list 101 in
Device(config-router-af) # distribute-list prefix-list 102 in ethernet 0/0
```

**Related Commands**

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

<i>access-list-number</i>   <i>access-list-name</i>	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.
<i>interface-name</i>	(Optional) Name of a particular interface. The <i>interface-name</i> argument cannot be used in address-family configuration mode.
<i>routing-process</i>	(Optional) Name of a particular routing process, or the <b>static</b> or <b>connected</b> keyword.
<i>as-number</i>	(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 <i>access-list-name</i> argument was added.
12.0(7)T	Address family configuration mode was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	Address-family topology configuration mode was added.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

### Usage Guidelines

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

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



#### Note

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

**Release 12.2(33)SRB**

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

**Examples**

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

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

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

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

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

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

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

**Related Commands**

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



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

## fast-reroute load-sharing disable

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

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

### Syntax Description

<b>level-1</b>	Specifies Level 1 packets.
<b>level-2</b>	Specifies Level 2 packets.

### Command Default

Load sharing of prefixes is enabled by default.

### Command Modes

Router configuration (config-router)

### Command History

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

### Usage Guidelines

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

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

### Examples

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

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

### Related Commands

Command	Description
<b>router isis</b>	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	Parameter	Description
	<b>level-1</b>	Enables per-prefix FRR of Level 1 packets.
	<b>level-2</b>	Enables per-prefix FRR of Level 2 packets.
	<b>all</b>	Enables FRR of all primary paths.
	<b>route-map</b>	Specifies the route map for selecting primary paths for protection.
	<i>route-map-name</i>	Route map name.

**Command Default** Fast Reroute per prefix is disabled.

**Command Modes** Router configuration (config-router)

Command History	Release	Modification
	15.1(2)S	This command was introduced.
	Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
	15.2(2)SNI	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

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

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

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

## Examples

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

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

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>router isis</b>	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

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

## Command Default

Tiebreaking is enabled by default.

## Command Modes

Router configuration (config-router)

## Command History

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

## Usage Guidelines

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

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

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

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

---

**Examples**

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

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

---

**Related Commands**

Command	Description
<b>router isis</b>	Enables the IS-IS routing protocol and specifies an IS-IS process.

# echo

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

**echo**  
**no echo**

**Syntax Description** This command has no arguments or keywords.

**Command Default** BFD echo mode is disabled.

**Command Modes** BFD configuration (config-bfd)

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

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

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



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



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

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

## Examples

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

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

Related Commands	Command	Description
	<b>interval (BFD)</b>	Configures the transmit and receive intervals between BFD packets.

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



# include-tcp-options

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

## include-tcp-options

**Command Default** This option is disabled.

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

Command History	Release	Modification
	16.12.1	This command was introduced.

**Usage Guidelines** This option must be configured on both devices.

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

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

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

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

Related Commands	Command	Description
	<b>accept-lifetime</b>	Sets the time period during which the authentication key on a key chain is received as valid.
	<b>ip authentication key-chain eigrp</b>	Enables authentication of EIGRP packets.
	<b>key</b>	Identifies an authentication key on a key chain.
	<b>key chain <i>key-name</i> tcp</b>	Defines a TCP-AO authentication key-chain needed to enable authentication for routing protocols.
	<b>key-string (authentication)</b>	Specifies the authentication string for a key.
	<b>send-lifetime</b>	Sets the time period during which an authentication key on a key chain is valid to be sent.
	<b>show key chain</b>	Displays authentication key information.

## interval (BFD)

To configure the transmit and receive intervals between Bidirectional 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

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

### Command Default

No session parameters are set.

### Command Modes

BFD configuration (config-bfd)

### Command History

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

### Usage Guidelines

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

### Examples

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

```
Router(config)# bfd-template single-hop node1
Router(bfd-config)# interval min-tx 120 min-rx 100 multiplier 3
```

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

```
Router(config)# bfd-template multi-hop template1
Router(bfd-config)# interval min-tx 200 min-rx 200 multiplier 3
```

#### Related Commands

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

<i>network-number</i>	Number of the network.
-----------------------	------------------------

## Command Default

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

## Command Modes

Global configuration (config#)

## Command History

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

## Usage Guidelines

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

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

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

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

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

## Examples

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

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

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

```
ip default-network 10.140.0.0
```

**Related Commands**

Command	Description
<b>show ip route</b>	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

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

## Command Default

The router discovery mechanism is not configured.

## Command Modes

Global configuration (config)

## Command History

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

## Usage Guidelines

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

## Examples

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

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

## Related Commands

Command	Description
<b>ip host</b>	Defines static hostname-to-address mappings in the DNS hostname cache for a DNS view.
<b>ip route</b>	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. To disable local policy routing, use the **no** form of this command.

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

<b>Syntax Description</b>	<i>map-tag</i>	Name of the route map to use for local policy routing. The name must match a <i>map-tag</i> value specified by a <b>route-map</b> command.
---------------------------	----------------	--

**Command Default** Packets that are generated by the router are not policy routed.

**Command Modes** Global configuration

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

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

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

## Examples

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

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

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

Command	Description
<b>match length</b>	Bases policy routing on the Level 3 length of a packet.
<b>route-map (IP)</b>	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
<b>set default interface</b>	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.
<b>set interface</b>	Indicates where to output packets that pass a match clause of route map for policy routing.
<b>set ip default next-hop</b>	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.
<b>set ip next-hop</b>	Indicates where to output packets that pass a match clause of a route map for policy routing.
<b>show ip local policy</b>	Displays the route map used for local policy routing.



# ip policy route-map

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

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

<b>Syntax Description</b>	<i>map-tag</i>	Name of the route map to use for policy routing. The name must match a <i>map-tag</i> value specified by a <b>route-map</b> command.
---------------------------	----------------	--

**Command Default** No policy routing occurs on the interface.

**Command Modes** Interface configuration (config-if)

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

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

The **ip policy route-map** command identifies a route map to use for policy routing. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*--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 *set actions*--the particular policy routing actions to perform if the criteria enforced by the **match** commands are met. The **no ip policy route-map** command deletes the pointer to the route map.

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

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

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

## Examples

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

```
interface serial 0
```

## ip policy route-map

```

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
<b>match ip address</b>	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.
<b>match length</b>	Bases policy routing on the Level 3 length of a packet.
<b>route-map (IP)</b>	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
<b>set default interface</b>	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.
<b>set interface</b>	Indicates where to output packets that pass a match clause of route map for policy routing.
<b>set ip default next-hop</b>	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.
<b>set ip next-hop</b>	Indicates where to output packets that pass a match clause of a route map for policy routing.

# ip route

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

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

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

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

```
no ip route
```

## Syntax Description

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

<b>tag</b> <i>tag</i>	(Optional) Tag value that can be used as a “match” value for controlling redistribution via route maps.
-----------------------	---

**Syntax Description****Syntax Description**

<i>prefix</i>	IP route prefix for the destination.
<i>mask</i>	Prefix mask for the destination.
<b>segment-routing policy</b>	Configures the segment routing policy.
<i>policy name</i>	Name of the segment routing policy.

**Command Default**

No static routes are established.

**Command Modes**

Global configuration (config)

**Command History**

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

**Usage Guidelines**

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

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

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

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

route, specify an administrative distance greater than 100. Static routes have a default administrative distance of 1.

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

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

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

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

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

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

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

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

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

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

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

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

Specifying a numerical next hop that is on a directly connected interface will prevent the router from using proxy ARP. However, if the interface with the next hop goes down and the numerical next hop can be reached

through a recursive route, you may specify both the next hop and interface (for example, `ip route 0.0.0.0 0.0.0.0 ethernet 1/2 10.1.2.3`) with a static route to prevent routes from passing through an unintended interface.



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

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

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

### Recursive Static Routing

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

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

```
ip route 192.168.1.1 255.255.255.255 10.0.0.2
```

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

The following example defines a valid recursive IPv4 static route:

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

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

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

It is not normally useful to manually configure a self-recursive static route, although it is not prohibited. However, a recursive static route that has been inserted in the IPv4 routing table may become self-recursive as a result of some transient change in the network learned through a dynamic routing protocol. If this situation occurs, the fact that the static route has become self-recursive will be detected and the static route will be

removed from the IPv4 routing table, although not from the configuration. A subsequent network change may cause the static route to no longer be self-recursive, in which case it will be re-inserted in the IPv4 routing table.



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

## Examples

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

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



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

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

```
ip route 172.31.0.0 255.255.0.0 172.31.6.6
```

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

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

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

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

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

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

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

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

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

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

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

## Examples

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

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

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

## Related Commands

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



# ip route profile

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

**ip route profile commandp route profile**  
**no ip route profile**

## Syntax Description

This command has no arguments or keywords.

## Command Default

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

## Command Modes

Global configuration

## Command History

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

## Usage Guidelines

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

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

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

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

Routing table statistics are collected for the following events:

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

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

---

**Examples**

The following example enables the collection of routing table statistics:

```
ip route profile
```

---

**Related Commands**

Command	Description
<b>show ip route profile</b>	Displays routing table change statistics.

## ip route static adjust-time

To change the time interval for IP static route adjustments during convergence, use the **ip route static adjust-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*

<b>Syntax Description</b>	<i>seconds</i>	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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.0(29)S	This command was introduced.
	12.3(10)	This command was integrated into Cisco IOS Release 12.3(10).
	12.3(11)T	This command was integrated into Cisco IOS Release 12.3(11)T.

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

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

### Examples

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

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

To remove the 30-second adjusted time interval and reinstate the default 60-second value, enter the **no ip route static adjust-time** command:

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

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show ip route</b>	Displays the current state of the routing table.

## ip route static bfd

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

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

### Syntax Description

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

### Command Default

No static route BFD neighbors are specified.

### Command Modes

Global configuration (config)

### Command History

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

## Usage Guidelines

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

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

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

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

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

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

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

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

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

1. Enable BFD timers on the SVI.

```
bfd interval milliseconds min_rx milliseconds multiplier multiplier-value
```

2. Enable BFD for the static IP route

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

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

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

```
bfd interval milliseconds min_rx milliseconds multiplier multiplier-value
```

## Examples

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

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

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

**ip route static bfd**

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

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

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

**Related Commands**

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

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

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

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

Syntax Description		
	<b>all</b>	(Optional) Installs all recursive static routes into the RIB.
	<b>multicast</b>	(Optional) Installs recursive static routes into multicast topologies.
	<b>route-map</b> <i>map-name</i>	(Optional) Installs recursive static routes defined by the specified route map into the RIB.
	<b>topology</b> <i>topology-name</i>	(Optional) Installs recursive static routes into the specified topology.
	<b>vrf</b> <i>vrf-name</i>	(Optional) Installs recursive static routes into the specified virtual routing and forwarding (VRF) instance.

**Command Default** No recursive static routes are installed in the RIB.

**Command Modes** Global configuration (config)

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

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

## Examples

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

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

## Related Commands

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



# ip routing

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

**ip routing**  
**no ip routing**

**Syntax Description** This command has no arguments or keywords.

**Command Default** IP routing is enabled.

**Command Modes** Global configuration (config)

## Command History

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

## Usage Guidelines

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

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

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

## Examples

The following example enables IP routing:

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

# ip routing protocol purge interface

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

**ip routing protocol purge interface**  
**no ip routing protocol purge interface**

**Syntax Description** This command has no arguments or keywords.

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

**Command Modes** Global configuration (config)

## Command History

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

## Usage Guidelines

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

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

## Examples

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

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

## ipv6 local policy route-map

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

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

<b>Syntax Description</b>	<i>route-map-name</i>	Name of the route map to be used for local IPv6 PBR. The name must match a <i>route-map-name</i> value specified by the <b>route-map</b> command.
---------------------------	-----------------------	---

**Command Default** IPv6 packets are not policy routed.

**Command Modes** Global configuration (config#)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.3(7)T	This command was introduced.
	12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)S.
	12.2(33)SX14	This command was integrated into Cisco IOS Release 12.2(33)SX14.
	Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.
	15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

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

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

### Examples

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

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

**Related Commands**

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

# ipv6 policy route-map

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

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

## Syntax Description

<i>route-map-name</i>	Name of the route map to be used for PBR. The name must match the <i>map-tag</i> value specified by a <b>route-map</b> command.
-----------------------	---

## Command Default

Policy-based routing does not occur on the interface.

## Command Modes

Interface configuration (config-if)

## Command History

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

## Usage Guidelines

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

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

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

## Examples

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

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

## Related Commands

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

## ipv6 route static bfd

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

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

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

**Command Default** No static route BFDv6 neighbors are specified.

**Command Modes** Global configuration (config)

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

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

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

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

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

The following example converts the neighbor to unassociated mode:

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

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show ipv6 static</b>	Displays the current contents of the IPv6 routing table.



# isdn supp-service callRerouteing

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

**isdn supp-service callRerouteing**

---

## Syntax Description

This command has no arguments or keywords.

---

## Command Default

ISDN partial rerouting is not enabled.

## Command Modes

Interface configuration (config-if)

## Command History

---

### Release Modification

---

16.5.1 This command was introduced.

---

## Usage Guidelines

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

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

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

## Example

The following example enables ISDN partial rerouting on interface bri1:

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

## ipv6 route static resolve default

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

```
ipv6 route static resolve default
no ipv6 route static resolve default
```

**Syntax Description** This command has no arguments or keywords.

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

**Command Modes** Global configuration (config)

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

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

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

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

# key

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

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

## Syntax Description

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

## Command Default

No key exists on the key chain.

## Command Modes

Key-chain configuration (config-keychain)

## Command History

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

## Usage Guidelines

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

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

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

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

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

## Examples

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

```
Router(config)# interface ethernet 0
Router(config-if)# ip rip authentication key-chain chain1
```

```

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

```

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

```

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

```

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

```

Router(config)# eigrp virtual-name
Router(config-router)# service-family ipv4 autonomous-system 4453
Router(config-router-sf)# network 10.0.0.0
Router(config-router-sf)# sf-interface ethernet0/0
Router(config-router-sf-interface)# authentication key-chain trees
Router(config-router-sf-interface)# authentication mode md5
Router(config-router-sf-interface)# exit
Router(config-router-sf)# exit
Router(config-router)# exit
Router(config)# key chain chain1

```

```

Router(config-keychain)# key 1
Router(config-keychain-key)# key-string key1
Router(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 14:00:00 Jan 25 1996 duration 3600
Router(config-keychain-key)# exit
Router(config-keychain)# key 2
Router(config-keychain-key)# key-string key2
Router(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 15:00:00 Jan 25 1996 duration 3600

```

**Related Commands**

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

# key chain

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

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

## Syntax Description

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

## Command Default

No key chain exists.

## Command Modes

Global configuration (config)

## Command History

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

## Usage Guidelines

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

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

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

## Examples

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

```
Router(config)# interface ethernet 0
Router(config-if)# ip rip authentication key-chain chain1
Router(config-if)# ip rip authentication mode md5
!
Router(config)# router rip
```

```

Router(config-router)# network 172.19.0.0
Router(config-router)# version 2
!
Router(config)# key chain chain1
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string key1
Router(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 14:00:00 Jan 25 1996 duration 3600
Router(config-keychain-key)# exit
Router(config-keychain)# key 2
Router(config-keychain-key)# key-string key2
Router(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 15:00:00 Jan 25 1996 duration 3600

```

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

```

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

```

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

```

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

```

```

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

```

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

```

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

```

## Related Commands

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



# key-string (authentication)

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

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

<b>Syntax Description</b>	<i>text</i> Authentication string that must be sent and received in the packets using the routing protocol being authenticated. The string can contain from 1 to 80 uppercase and lowercase alphanumeric characters.
---------------------------	--

**Command Default** No authentication string for a key exists.

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

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

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

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

## Examples

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

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

## key-string (authentication)

```

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

<i>interface- type</i>	Interface type.
<i>interface- number</i>	Interface number.

### Command Default

No match interfaces are defined.

### Command Modes

Route-map configuration (config-route-map)

### Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(2)S	This command was integrated into Cisco IOS Release 15.1(2)S.

### Usage Guidelines

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

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

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

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

### Examples

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

## match interface (IP)

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

## Related Commands

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

<i>access-list-number</i> ..	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.
<i>access-list-name</i> ...	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.
<b>prefix-list</b>	Distributes routes based on a prefix list.
<i>prefix-list-name</i> ...	Name of a specific prefix list. The ellipsis indicates that multiple values can be entered.

## Command Default

No access list numbers or prefix lists are specified.

## Command Modes

Route-map configuration (config-route-map)

## Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(2)S	This command was integrated into Cisco IOS Release 15.1(2)S.

## Usage Guidelines

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *access-list-number*, *access-list-name*, or *prefix-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 **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 *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 **ip policy route-map** interface configuration command, in addition to the **route-map** global configuration command, and the **match** and **set** route-map configuration commands. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *matchcriteria*--the conditions under which policy routing occurs. The **set** commands specify the *setactions*--the particular routing actions to perform if the criteria enforced by the **match** commands are met. You might want to policy route packets based on their source, for example, using an access list.

## Examples

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

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

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

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

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

```

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

```

**Related Commands**

Command	Description
<b>ip local policy route-map</b>	Identifies a route map to use for policy routing on an interface.
<b>ip policy route-map</b>	Identifies a route map to use for policy routing on an interface.
<b>match as-path</b>	Matches a BGP autonomous system path access list.
<b>match community</b>	Matches a BGP community.
<b>match interface (IP)</b>	Distributes any routes that have their next hop out one of the interfaces specified.
<b>match ip next-hop</b>	Redistributes any routes that have a next hop router address passed by one of the access lists specified.
<b>match ip route-source</b>	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
<b>match length</b>	Bases policy routing on the Level 3 length of a packet.
<b>match metric (IP)</b>	Redistributes routes with the metric specified.
<b>match route-type (IP)</b>	Redistributes routes of the specified type.
<b>match tag</b>	Redistributes routes in the routing table that match the specified tags.
<b>route-map (IP)</b>	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
<b>set as-path</b>	Modifies an autonomous system path for BGP routes.
<b>set automatic-tag</b>	Automatically computes the tag value.
<b>set community</b>	Sets the BGP communities attribute.
<b>set default interface</b>	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.
<b>set interface</b>	Indicates where to output packets that pass a match clause of a route map for policy routing.
<b>set ip default next-hop</b>	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.
<b>set ip next-hop</b>	Indicates where to output packets that pass a match clause of a route map for policy routing.

<b>Command</b>	<b>Description</b>
<b>set level (IP)</b>	Indicates where to import routes.
<b>set local-preference</b>	Specifies a preference value for the autonomous system path.
<b>set metric (BGP, OSPF, RIP)</b>	Sets the metric value for a routing protocol.
<b>set metric-type</b>	Sets the metric type for the destination routing protocol.
<b>set next-hop</b>	Specifies the address of the next hop.
<b>set tag (IP)</b>	Sets a tag value of the destination routing protocol.
<b>set weight</b>	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 **match ip next-hop** command in route-map configuration mode. To remove the next hop entry, use the **no** form of this command.

```
match ip next-hop {access-list-numberaccess-list-name} [{... access-list-number | ...  
access-list-name}]
```

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

<b>Syntax Description</b>	<i>access-list-number</i> <i>access-list-name</i>	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)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	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 *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.

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

**Examples**

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

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

**Related Commands**

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

<i>access-list-number</i>	(Optional) Number of a standard access list. The range is from 1 to 199.
<i>expanded-access-list</i>	(Optional) Number of an expanded access list. The range is from from 1300 to 1999.
<i>access-list-name</i>	(Optional) Name of a standard access list.
<b>prefix-list</b> <i>name</i>	(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 **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.

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

### Examples

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

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

### Related Commands

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

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

## match ip route-source

To match routes that have been advertised by routers and access servers at the address specified by the access lists, use the **match ip route-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

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

### Command Default

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

### Command Modes

Route-map configuration (config-route-map)

### Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 and implemented on Cisco ASR 1000 Series Aggregation Services Routers.

### Usage Guidelines

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

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

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



# match ipv6 address

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

```
match ipv6 address {prefix-list prefix-list-name access-list-name}
no match ipv6 address
```

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

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

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

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

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

## match ipv6 address

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

### Examples

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

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

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

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

### Related Commands

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

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

# match length

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

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

## Syntax Description

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

## Command Default

No policy routing occurs on the length of a packet.

## Command Modes

Route-map configuration (config-route-map)

## Command History

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

## Usage Guidelines

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

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

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

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

**Examples**

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

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

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

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

**Related Commands**

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

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

## match metric (IP)

To redistribute routes 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		
<i>metric-value</i>		Internal route metric, which can be an Enhanced Interior Gateway Routing Protocol (EIGRP) five-part metric. The range is from 1 to 4294967295.
<b>external</b>		External protocol associated with a route and interpreted by a source protocol.
+ <i> deviation-number</i>		(Optional) A standard deviation number that will offset the number configured for the <i>metric-value</i> argument. The <i>deviation-number</i> argument can be any number. There is no default.  <b>Note</b> 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 <b>external</b> and +-keywords and <i>deviation-number</i> 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 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 a second route map section with an explicit match specified.



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

## Examples

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

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

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

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

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

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

## Related Commands

Command	Description
<b>match as-path</b>	Matches a BGP autonomous system path access list.
<b>match community</b>	Matches a BGP community.
<b>match interface (IP)</b>	Distributes any routes that have their next hop out one of the interfaces specified.
<b>match ip address</b>	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.
<b>match ip next-hop</b>	Redistributes any routes that have a next hop router address passed by one of the access lists specified.
<b>match ip route-source</b>	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
<b>match route-type (IP)</b>	Redistributes routes of the specified type.
<b>match tag</b>	Redistributes routes in the routing table that match the specified tags.



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

<b>local</b>	Locally generated Border Gateway Protocol (BGP) routes.
<b>internal</b>	Open Shortest Path First (OSPF) intra-area and interarea routes or Enhanced Interior Gateway Routing Protocol (EIGRP) internal routes.
<b>external [type-1 type-2]</b>	OSPF external routes, or EIGRP external routes. For OSPF, the <b>externaltype-1</b> keyword matches only Type 1 external routes and the <b>externaltype-2</b> keyword matches only Type 2 external routes.
<b>level-1</b>	Intermediate System-to-Intermediate System (IS-IS) Level 1 routes.
<b>level-2</b>	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 <b>local</b> and <b>external [type-1   type-2]</b> keywords were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

### Usage Guidelines

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

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

A route map can have several parts. Any route that does not match at least one **match** clause relating to a **route-map** command will be ignored; that is, the route will not be advertised for outbound route maps and

will not be accepted for inbound route maps. If you want to modify only some data, you must configure second route map section with an explicit match specified.

## Examples

The following example redistributes internal routes:

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

## Related Commands

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

# match tag

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

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

## Syntax Description

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

## Command Default

No match tag values are defined.

## Command Modes

Route-map configuration (config-route-map)

## Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was implemented on Cisco ASR 1000 Series Aggregation Services Routers.
15.1(2)S	This command was integrated into Cisco IOS Release 15.1(2)S.
15.2(2)S	This command was modified. The <i>tag-value-dotted-decimal</i> argument was added to support tag values in dotted-decimal format.
Cisco IOS XE Release 3.6S	This command was modified. The <i>tag-value-dotted-decimal</i> argument was added to support tag values in dotted-decimal format.

## Usage Guidelines

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

## Examples

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

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

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

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

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

# match tag list

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

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

## Syntax Description

<i>list-name</i>	Name of route tag lists.
------------------	--------------------------

## Command Default

No match tag lists are defined.

## Command Modes

Route-map configuration (config-route-map)

## Command History

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

## Usage Guidelines

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

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



### Note

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

## Examples

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

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

## Related Commands

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

# match track

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

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

<b>Syntax Description</b>	<i>track-object-number</i> Number of the stub object that you want to track. The range is from 1 to 1000.
---------------------------	---

<b>Command Default</b>	Stub object is not tracked.
------------------------	-----------------------------

<b>Command Modes</b>	Route-map configuration (config-route-map)
----------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	15.4(3)M	This command was introduced.
	Cisco IOS XE Release 3.13S	This command was integrated into Cisco IOS XE Release 3.13S.

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

## Example

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

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

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

# maximum-paths

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

**maximum-paths** *number-of-paths*

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

## Syntax Description

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

## Command Default

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

## Command Modes

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

Router configuration (config-router)

## Command History

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

## Usage Guidelines

### Release 12.2(33)SRB

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

## Examples

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

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



# monitor peer bfd

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

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

<b>Syntax Description</b>	<b>local interface</b> <i>interface-type</i> (Optional) Specifies the local interface for the source address to use when locating a BFD configuration.
---------------------------	--

**Command Default** Pseudowire fast-failure detection is disabled.

**Command Modes**

- Interface configuration (config-if)
- Pseudowire class configuration (config-pw-class)
- Template configuration (config-template)

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

## Examples

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

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

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

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

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

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

**Related Commands**

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

## named-ordering-route-map enable

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

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

---

**Syntax Description**

This command has no arguments or keywords.

---

**Command Default**

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

---

**Command Modes**

Global configuration (config)

---

**Command History**

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

---

**Examples**

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

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

# nsf

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

**nsf** [**enforce global**]

**nsf** [{{**cisco** | **ietf**} | **interface wait** *seconds* | **interval** *minutes* | **t3** [{{**adjacency** | **manual** *seconds*}}]]

**no nsf**

## Syntax Description

<b>enforce global</b>	(Optional) Cancels OSPF NSF restart when non-NSF-aware neighbors are detected.
<b>cisco</b>	Specifies the Cisco proprietary IS-IS NSF method of checkpointing if the active RP fails over.
<b>ietf</b>	Specifies the IETF IS-IS NSF method of protocol modification if the active RP fails over.
<b>interface wait</b> <i>seconds</i>	(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.
<b>interval</b> <i>minutes</i>	(Optional) Specifies how long to wait after a route processor stabilizes before restarting; valid values are from 0 to 1440 minutes.
<b>t3 adjacency</b>	(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.
<b>t3 manual</b> <i>seconds</i>	(Optional) Specifies the time to wait after the NSF database synchronizes before informing other nodes to remove the restarting node from consideration as a transit; valid values are from 5 to 3600 seconds.

## Command Default

The default settings are as follows:

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

## Command Modes

Router configuration

## Command History

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

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

### Usage Guidelines

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

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



### Note

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

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

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

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

The [`{cisco | ietf}`] interface **waitseconds** | 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 **bgp graceful-restart** router configuration command to enable the graceful restart capability.

### EIRGP NSF Guidelines

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

### IS-IS NSF Guidelines

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

Use these two keywords when configuring IS-IS NSF:

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

### OSPF NSF Guidelines

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

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

### Examples

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

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

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

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

### Related Commands

Command	Description
<b>router</b>	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** **command**  
**passive-interface** [**default**] **i** *interface-type* *interface-number*  
**no passive-interface** *interface-type* *interface-number*

## Syntax Description

<b>default</b>	(Optional) Causes all interfaces to become passive.
<i>interface-type</i>	Interface type.
<i>interface-number</i>	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 <b>default</b> 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 **no****passive-interface** command. The **default** keyword is useful in Internet service provider (ISP) and large enterprise networks where many of the distribution routers have more than 200 interfaces.

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](http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080093f0a.shtml).

## Examples

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

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

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

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

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

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



# platform bfd allow-svi

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

## platformbfd allow-svi

### Syntax Description

This command has no arguments or keywords.

### Command Default

BFD configuration on VLAN SVIs is not allowed.

### Command Modes

Global configuration (config)#

### Command History

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

### Usage Guidelines

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

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



### Note

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

### Examples

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

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

### Related Commands

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

# platform bfd enable-offload

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

**platform bfd enable-offload**  
**no platform bfd enable-offload**

**Syntax Description** This command has no arguments or keywords

**Command Default** Command is disabled.

**Command Modes** Global configuration (config)#

## Command History

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

## Usage Guidelines

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

## Examples

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

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

# platform cloudsec padding-fixup

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

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

## Syntax Description

**padding-fixup** Specifies the fixup for the small CloudSec packets with padding length.

**dst-udp-port** Specifies the UDP destination port numbers for CloudSec packets.

*1st port number* Specifies the 1st UDP destination port.

Valid values are from 1024 to 49151.

*2nd port number* (Optional) Specifies the 2nd UDP destination port.

Valid values are from 1024 to 49151.

*3rd port number* (Optional) Specifies the 3rd UDP destination port.

Valid values are from 1024 to 49151.

**debug** Specifies the CloudSec debug.

## Command Default

Command is disabled.

## Command Modes

Global configuration (config)#

## Command History

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

## Usage Guidelines

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

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

## Examples

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

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

**Related Commands**

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

# recv-id

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

**recv-id** *ID*

## Syntax Description

<i>ID</i>	Specifies the receive identifier. An integer between 0 to 255.
-----------	--

## Command Default

No key chain exists.

## Command Modes

Key chain key configuration (config-keychain-key)

## Command History

Release	Modification
16.12.1	This command was introduced.

## Usage Guidelines

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

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

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

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

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

## Related Commands

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

## redistribute (IP)

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

```

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

```

### Syntax Description

<i>protocol</i>	<p>Source protocol from which routes are being redistributed. It can be one of the following keywords: <b>application</b>, <b>bgp</b>, <b>connected</b>, <b>eigrp</b>, <b>isis</b>, <b>mobile</b>, <b>ospf</b>, <b>rip</b>, <b>nhrp</b>, or <b>static [ip]</b>.</p> <p>The <b>static [ip]</b> keyword is used to redistribute IP static routes. The optional <b>ip</b> keyword is used when redistributing into the Intermediate System-to-Intermediate System (IS-IS) protocol.</p> <p>The <b>application</b> keyword is used to redistribute an application from one routing domain to another. In Cisco IOS XE Release 3.12S and Cisco IOS Release 15.4(3)M, you can redistribute more than one application to different routing protocols such as IS-IS, OSPF, Border Gateway Protocol (BGP), Enhanced Interior Gateway Routing Protocol (EIGRP) and Routing Information Protocol (RIP).</p> <p>The <b>connected</b> 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.</p>
-----------------	--

<i>process-id</i>	<p>(Optional) For the <b>application</b> keyword, this is the name of an application.</p> <p>For the <b>bgp</b> or <b>eigrp</b> keyword, this is an autonomous system number, which is a 16-bit decimal number.</p> <p>For the <b>isis</b> keyword, this is an optional <i>tag</i> value that defines a meaningful name for a routing process. Creating a name for a routing process means that you use names when configuring routing. You can configure a router in two routing domains and redistribute routing information between these two domains.</p> <p>For the <b>ospf</b> 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.</p> <p>For the <b>nhrp</b> keyword, this is an appropriate NHRP process ID from which routes are to be redistributed. This identifies the routing process. This value takes the form of a nonzero decimal number.</p> <p>For the <b>rip</b> keyword, no <i>process-id</i> value is needed.</p> <p>For the <b>application</b> keyword, this is the name of an application.</p> <p>By default, no process ID is defined.</p>
<b>level-1</b>	Specifies that, for IS-IS, Level 1 routes are redistributed into other IP routing protocols independently.
<b>level-1-2</b>	Specifies that, for IS-IS, both Level 1 and Level 2 routes are redistributed into other IP routing protocols.
<b>level-2</b>	Specifies that, for IS-IS, Level 2 routes are redistributed into other IP routing protocols independently.
<i>autonomous-system-number</i>	<p>(Optional) Autonomous system number for the redistributed route. The range is from 1 to 65535.</p> <ul style="list-style-type: none"> <li>• In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, 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.</li> <li>• 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.</li> </ul> <p>For more details about autonomous system number formats, see the <b>router bgp</b> command.</p>

<b>metric</b> <i>metric-value</i>	<p>(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.</p> <p>(Optional) When redistributing from one NHRP process to another routing process on the same router, the metric will be carried through from one process to the other if no metric value is specified. The default value is 0.</p>
<b>metric transparent</b>	(Optional) Causes RIP to use the routing table metric for redistributed routes as the RIP metric.
<b>metric-type</b> <i>type value</i>	<p>(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:</p> <ul style="list-style-type: none"> <li>• <b>1</b>—Type 1 external route</li> <li>• <b>2</b>—Type 2 external route</li> </ul> <p>If a <b>metric-type</b> is not specified, the Cisco IOS software adopts a Type 2 external route.</p> <p>For IS-IS, it can be one of two values:</p> <ul style="list-style-type: none"> <li>• <b>internal</b>—IS-IS metric that is &lt; 63.</li> <li>• <b>external</b>—IS-IS metric that is &gt; 64 &lt; 128.</li> </ul> <p>The default is <b>internal</b>.</p>
<b>match</b> { <b>internal</b>   <b>external1</b>   <b>external2</b> }	<p>(Optional) Specifies the criteria by which OSPF routes are redistributed into other routing domains. It can be one of the following:</p> <ul style="list-style-type: none"> <li>• <b>internal</b>—Routes that are internal to a specific autonomous system.</li> <li>• <b>external 1</b>—Routes that are external to the autonomous system, but are imported into OSPF as Type 1 external routes.</li> <li>• <b>external 2</b>—Routes that are external to the autonomous system, but are imported into OSPF as Type 2 external routes.</li> </ul> <p>The default is <b>internal</b>.</p>



<b>tag</b> <i>tag-value</i>	(Optional) Specifies the 32-bit decimal value attached to each external route. This is not used by OSPF itself. It may be used to communicate information between Autonomous System Boundary Routers (ASBRs). If none is specified, the remote autonomous system number is used for routes from BGP and Exterior Gateway Protocol (EGP); for other protocols, zero (0) is used.
<b>route-map</b>	(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.
<i>map-tag</i>	(Optional) Identifier of a configured route map.
<b>registered</b>	(Optional) Limit redistribution to registered NHRP routes.
<b>resolved</b>	(Optional) Limit redistribution to resolved NHRP routes.
<b>summary</b>	(Optional) Limit redistribution to NHRP summary routes.
<b>subnets</b>	(Optional) For redistributing routes into OSPF, the scope of redistribution for the specified protocol. By default, no subnets are defined.
<b>nssa-only</b>	(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**

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

Release	Modification
12.2(33)SRB	This command was modified. Address family topology support under EIGRP was added.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX.
12.0(32)S12	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(24)T	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.3	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SX11	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 <b>nssa-only</b> keyword was added.
12.2(33)SRE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
15.1(1)SG	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
Cisco IOS XE Release 3.3SG	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers
Cisco IOS XE Release 3.9S	This command was modified. The <b>subnets</b> keyword was deprecated for OSPF classful redistribution.
15.2(1)E	This command was integrated into Cisco IOS Release 15.2(1)E.
Cisco IOS XE Release 3.12S	This command was modified. Support for redistribution of more than one application from one routing domain to another routing domain was added.
Cisco IOS XE Gibraltar 16.12.1x	Command is modified to include options for redistributing NHRP routes. The following keywords are added: <b>registered</b> , <b>resolved</b> , and <b>summary</b> .

## Using the no Form of the redistribute Command



### Caution

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

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

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

## Additional Usage Guidelines for the redistribute Command

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

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

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

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

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

advertised as the external metric in the redistribution destination process. (This is the only case in which the routing table metric will be preserved when routes are redistributed into OSPF.)

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




---

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

---

On a router internal to an NSSA area, the **nssa-only** keyword causes the originated type-7 NSSA LSAs to have their propagate (P) bit set to zero, which prevents area border routers from translating these LSAs into type-5 external LSAs. On an area border router that is connected to an NSSA and normal areas, the **nssa-only** keyword causes the routes to be redistributed only into the NSSA areas.

Routes configured with the **connected** keyword affected by this **redistribute** command are the routes not specified by the **network** router configuration command.

You cannot use the **default-metric** command to affect the metric used to advertise connected routes.




---

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

---

The default redistribution of Interior Gateway Protocol (IGP) or Exterior Gateway Protocol (EGP) into BGP is not allowed unless the **default-information originate** router configuration command is specified.

You can use the **redistribute nhrp process-id [metric metric-value][registered] [resolved] [summary] [route-map map-tag]** command to distribute all or specific NHRP routes. The routes that can be specified are registered, resolved, or summary routes. The keywords ‘registered’, ‘resolved’ and ‘summary’ are used to filter redistributed routes based on their origin. If none of these is specified, all NHRP routes are redistributed when redistribution from NHRP is configured.

Standard redistribution filtering mechanisms such as route-maps and tagging can also be used.

### Release 12.2(33)SRB

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

### 4-Byte Autonomous System Number Support

In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, and later releases, the Cisco implementation of 4-byte autonomous system numbers uses asplain—65538 for example—as the default regular expression match and output display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain format and the asdot format as described in RFC 5396. To change the default regular expression match and output display of 4-byte autonomous system numbers to asdot format, use the **bgp asnotation dot** command.

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

## Examples

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

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

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

```
Device(config)# router ospf 110
Device(config-router)# redistribute eigrp
```

The following example shows how to redistribute the specified EIGRP process routes into an OSPF domain. The EIGRP-derived metric will be remapped to 100 and RIP routes to 200.

```
Device(config)# router ospf 109
Device(config-router)# redistribute eigrp 108 metric 100 subnets
Device(config-router)# redistribute rip metric 200 subnets
```

The following example shows how to configure BGP routes to be redistributed into IS-IS. The link-state cost is specified as 5, and the metric type is set to external, indicating that it has lower priority than internal metrics.

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

The following example shows how to redistribute an application into an OSPF domain and specify a metric value of 5:

```
Device(config)# router ospf 4
Device(config-router)# redistribute application am metric 5
```

In the following example, network 172.16.0.0 will appear as an external LSA in OSPF 1 with a cost of 100 (the cost is preserved):

```
Device(config)# interface ethernet 0
Device(config-if)# ip address 172.16.0.1 255.0.0.0
Device(config-if)# exit
Device(config)# ip ospf cost 100
Device(config)# interface ethernet 1
Device(config-if)# ip address 10.0.0.1 255.0.0.0
!
Device(config)# router ospf 1
Device(config-router)# network 10.0.0.0 0.255.255.255 area 0
Device(config-if)# exit
Device(config-router)# redistribute ospf 2 subnet
Device(config)# router ospf 2
Device(config-router)# network 172.16.0.0 0.255.255.255 area 0
```

The following example shows how BGP routes are redistributed into OSPF and assigned the local 4-byte autonomous system number in asplain format. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)SXII, Cisco IOS XE Release 2.4, or a later release.

```
Device(config)# router ospf 2
Device(config-router)# redistribute bgp 65538
```

The following example shows how to remove the **connected metric 1000 subnets** options from the **redistribute connected metric 1000 subnets** command and leave the **redistribute connected** command in the configuration:

```
Device(config-router)# no redistribute connected metric 1000 subnets
```

The following example shows how to remove the **metric 1000** options from the **redistribute connected metric 1000 subnets** command and leave the **redistribute connected subnets** command in the configuration:

```
Device(config-router)# no redistribute connected metric 1000
```

The following example shows how to remove the **subnets** option from the **redistribute connected metric 1000 subnets** command and leave the **redistribute connected metric 1000** command in the configuration:

```
Device(config-router)# no redistribute connected subnets
```

The following example shows how to remove the **redistribute connected** command, and any of the options that were configured for the **redistribute connected** command, from the configuration:

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

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

```
Device(config)# router eigrp virtual-name
Device(config-router)# address-family ipv4 autonomous-system 1
Device(config-router-af)# topology base
Device(config-router-af-topology)# redistribute eigrp 6473 metric 1 1 1 1
```

The following example shows how to set and disable the redistributions in EIGRP configuration. Note that, in the case of EIGRP, the **no** form of the commands removes the entire set of **redistribute** commands from the running configuration.

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

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

```
Device# show running-config | section router eigrp 1
```

```
router eigrp 1
 network 0.0.0.0
```

The following example shows how to set and disable the redistributions in OSPF configuration. Note that the **no** form of the commands removes only the specified keywords from the **redistribute** command in the running configuration.

```

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

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

Device# show running-config | section router ospf 1

router ospf 1
 redistribute eigrp 2
 redistribute ospf 1
 redistribute bgp 1
 redistribute rip
 network 0.0.0.0

```

The following example shows how to remove only the route map filter from the redistribution in BGP; redistribution itself remains in force without a filter:

```

Device(config)# router bgp 65000
Device(config-router)# no redistribute eigrp 2 route-map x

```

The following example shows how to remove the EIGRP redistribution to BGP:

```

Device(config)# router bgp 65000
Device(config-router)# no redistribute eigrp 2

```

The following example shows how registered NHRP routes are redistributed into a BGP domain:

```

Router(config)# router bgp 109
Router(config-router)# redistribute nhrp 11 registered

```

#### Related Commands

Command	Description
<b>address-family (EIGRP)</b>	Enters address family configuration mode to configure an EIGRP routing instance.
<b>address-family ipv4 (BGP)</b>	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.
<b>address-family vpv4</b>	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.
<b>bgp asnotation dot</b>	Changes the default display and the regular expression match format of BGP 4-byte autonomous system numbers from asplain (decimal values) to dot notation.

Command	Description
<b>default-information originate (BGP)</b>	Allows the redistribution of network 0.0.0.0 into BGP.
<b>default-information originate (IS-IS)</b>	Generates a default route into an IS-IS routing domain.
<b>default-information originate (OSPF)</b>	Generates a default route into an OSPF routing domain.
<b>distribute-list out (IP)</b>	Suppresses networks from being advertised in updates.
<b>route-map (IP)</b>	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
<b>router bgp</b>	Configures the BGP routing process.
<b>router eigrp</b>	Configures the EIGRP address-family process.
<b>show route-map</b>	Displays all route maps configured or only the one specified.
<b>topology (EIGRP)</b>	Configures an EIGRP process to route IP traffic under the specified topology instance and enters address family topology configuration mode.



# route-map

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

```
route-map map-tag [{permit | deny}] [sequence-number] ordering-seq sequence-name
no route-map map-tag [{permit | deny}] [sequence-number] ordering-seq sequence-name
```

Syntax Description		
<i>map-tag</i>	Name for the route map.	
<b>permit</b>	(Optional) Permits only routes matching the route map to be forwarded or redistributed.	
<b>deny</b>	(Optional) Blocks routes matching the route map from being forwarded or redistributed.	
<i>sequence-number</i>	(Optional) Number that indicates the position a new route map will have in the list of route maps already configured with the same name.	
<b>ordering-seq</b> <i>sequence-name</i>	(Optional) Orders the route maps based on the string provided.	

**Command Default** Policy routing is not enabled and conditions for redistributing routes from one routing protocol to another routing protocol are not configured.

**Command Modes** Global configuration (config)

Command History	Release	Modification
	10.0	This command was introduced.
	12.3(7)T	This command was updated for use in configuring IPv6 policy-based routing (PBR).
	12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
	12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
	Cisco IOS XE Release 2.1	This command was implemented on Cisco ASR 1000 Series Aggregation Services Routers.
	12.2(33)SX14	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SX14.
	15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
	Cisco IOS XE Everest 16.6.1	The keyword <b>ordering-seq</b> was introduced in this release.

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

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

### Redistribution

Use the **route-map** global configuration command and the **match** and **set** route-map configuration commands to define the conditions for redistributing routes from one routing protocol to another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*--the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the *set actions*--the particular redistribution actions to be performed if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

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

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

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

The **redistribute** router configuration command uses the name specified by the *map-tag* argument to reference a route map. Multiple route maps may share the same map tag name.

If the match criteria are met for this route map, and the **permit** keyword is specified, the route is redistributed as controlled by the set actions. In the case of policy routing, the packet is policy routed. If the match criteria are not met, and the **permit** keyword is specified, the next route map with the same map tag is tested. If a route passes none of the match criteria for the set of route maps sharing the same name, it is not redistributed by that set.

If the match criteria are met for the route map and the **deny** keyword is specified, the route is not redistributed. In the case of policy routing, the packet is not policy routed, and no further route maps sharing the same map tag name will be examined. If the packet is not policy routed, the normal forwarding algorithm is used.

### Policy Routing

Another purpose of route maps is to enable policy routing. Use the **ip policy route-map** or **ipv6 policy route-map** command, in addition to the **route-map** command, and the **match** and **set** commands to define the conditions for policy routing packets. The **match** commands specify the conditions under which policy routing occurs. The **set** commands specify the routing actions to be performed if the criteria enforced by the **match** commands are met. You might want to policy route packets some way other than the obvious shortest path.

The *sequence-number* argument works as follows:

1. If no entry is defined with the supplied tag, an entry is created with the *sequence-number* argument set to 10.
2. If only one entry is defined with the supplied tag, that entry becomes the default entry for the following **route-map** command. The *sequence-number* argument of this entry is unchanged.

- If more than one entry is defined with the supplied tag, an error message is printed to indicate that the *sequence-number* argument is required.

If the **no route-map** *map-tag* command is specified (with no *sequence-number* argument), the whole route map is deleted.

## Examples

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

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

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

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

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

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

## Related Commands

Command	Description
<b>ip policy route-map</b>	Identifies a route map to use for policy routing on an interface.

Command	Description
<b>ipv6 policy route-map</b>	Configures IPv6 PBR on an interface.
<b>match as-path</b>	Matches a BGP autonomous system path access list.
<b>match community</b>	Matches a BGP community.
<b>match interface (IP)</b>	Distributes any routes that have their next hop on one of the specified interfaces.
<b>match ip address</b>	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.
<b>match ipv6 address</b>	Distributes IPv6 routes that have a prefix permitted by a prefix list or specifies an IPv6 access list to use to match packets for PBR for IPv6.
<b>match ip next-hop</b>	Redistributes any routes that have a next-hop router address passed by one of the specified access lists.
<b>match ip route-source</b>	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
<b>match length</b>	Bases policy routing on the Level 3 length of a packet.
<b>match metric (IP)</b>	Redistributes routes with the metric specified.
<b>match route-type (IP)</b>	Redistributes routes of the specified type.
<b>match tag</b>	Redistributes routes in the routing table that match the specified tags.
<b>router eigrp</b>	Configures the EIGRP address-family process.
<b>set as-path</b>	Modifies an autonomous system path for BGP routes.
<b>set automatic-tag</b>	Automatically computes the tag value.
<b>set community</b>	Sets the BGP communities attribute.
<b>set default interface</b>	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.
<b>set interface</b>	Indicates where to output packets that pass a match clause of a route map for policy routing.
<b>set ipv6 default next-hop</b>	Specifies an IPv6 default next hop to which matching packets will be forwarded.
<b>set ip default next-hop verify-availability</b>	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.

<b>Command</b>	<b>Description</b>
<b>set ip next-hop</b>	Indicates where to output packets that pass a match clause of a route map for policy routing.
<b>set ipv6 next-hop (PBR)</b>	Indicates where to output IPv6 packets that pass a match clause of a route map for PBR for IPv6.
<b>set level (IP)</b>	Indicates where to import routes.
<b>set local preference</b>	Specifies a preference value for the autonomous system path.
<b>set metric (BGP, OSPF, RIP)</b>	Sets the metric value for a routing protocol.
<b>set metric type</b>	Sets the metric type for the destination routing protocol.
<b>set next-hop</b>	Specifies the address of the next hop.
<b>set tag (IP)</b>	Sets a tag value of the destination routing protocol.
<b>set weight</b>	Specifies the BGP weight for the routing table.
<b>show route-map</b>	Displays all route maps configured or only the one specified.

## route-tag list

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

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

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

### Syntax Description

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

### Command Default

No route tag list is configured.

### Command Modes

Global configuration (config)

### Command History

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

### Usage Guidelines

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

### Examples

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

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

### Related Commands

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

## route-tag notation

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

**route-tag notation dotted-decimal**  
**no route-tag notation dotted-decimal**

<b>Syntax Description</b>	<b>dotted-decimal</b> Enables the display of route tag values in dotted-decimal format.
---------------------------	---

**Command Default** Tag values are displayed as plain decimals.

**Command Modes** Global configuration (config)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	15.2(2)S	This command was introduced.
	Cisco IOS XE Release 3.6S	This command was integrated into Cisco IOS XE Release 3.6S.
	15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.

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

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

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

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>eigrp default-route-tag</b>	Sets a default route tag for all internal EIGRP routes.
	<b>match tag</b>	Filters routes that match specified route tags.
	<b>set tag (IP)</b>	Sets a tag value for routes.
	<b>show ip route</b>	Displays contents of the IPv4 routing table.
	<b>show ipv6 route</b>	Displays contents of the IPv6 routing table.

Command	Description
<b>show route-map</b>	Displays information about static and dynamic route maps.
<b>show route-tag list</b>	Displays information about route tag lists configured on the device.



# routing dynamic

To enable the router to pass routing updates to other routers through an interface, use the **routingdynamic** command in interface configuration mode. To disable the passing of routing updates through an interface, use the **no** form of this command.

**routing dynamic**  
**no routing dynamic**

**Syntax Description** This command has no arguments or keywords.

**Command Default** Asynchronous interfaces: No routing updates are passed. All other interface types: Routing updates are passed.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.3(11)T	This command was introduced. This command replaces the <b>asynctdefaultrouting</b> command.

**Usage Guidelines** Use the **routingdynamic** command to control the passing of routing updates over an interface. Issuing the **noroutingdynamic** command flags the interface to indicate that routing updates should not be sent out of it.

The routing protocol must recognize the flag for this command to work as intended. The **routingdynamic** command sets and clears the flag; it does not enforce routing protocol conformance.

## Examples

The following example enables routing over asynchronous interface 0:

```
interface async 0
  routing dynamic
```

The following example disables routing over serial interface 2/0:

```
interface serial 2/0
  no routing dynamic
```

Related Commands	Command	Description
	<b>async dynamic routing</b>	Enables manually configured routing on an asynchronous interface.
	<b>passive-interface</b>	Disables sending routing updates on an interface.





## IP Routing Protocol-Independent Commands: S through T

---

- [send-lifetime](#), on page 157
- [send-id](#), on page 160
- [set automatic-tag](#), on page 162
- [set default interface](#), on page 164
- [set interface](#), on page 167
- [set ip default next-hop](#), on page 170
- [set ip default next-hop verify-availability](#), on page 172
- [set ip global](#), on page 173
- [set ip next-hop](#), on page 175
- [set ip next-hop verify-availability](#), on page 178
- [set ip vrf](#), on page 182
- [set ipv6 default next-hop](#), on page 184
- [set ipv6 next-hop \(PBR\)](#), on page 187
- [set ipv6 precedence](#), on page 189
- [set level \(IP\)](#), on page 191
- [set local-preference](#), on page 193
- [set metric \(BGP-OSPF-RIP\)](#), on page 195
- [set metric-type](#), on page 197
- [set next-hop](#), on page 199
- [set tag \(IP\)](#), on page 201
- [set vrf next-hop verify-availability](#), on page 203
- [show bfd drops](#), on page 206
- [show bfd neighbors](#), on page 208
- [show bfd summary](#), on page 219
- [show dampening interface](#), on page 221
- [show fm ipv6 pbr all](#), on page 223
- [show fm ipv6 pbr interface](#), on page 224
- [show interface dampening](#), on page 225
- [show ip cef platform](#), on page 227
- [show ip cache policy](#), on page 229
- [show ip local policy](#), on page 231

- [show ip policy](#), on page 233
- [show ip protocols](#), on page 235
- [show ip route](#), on page 242
- [show ip route loops](#), on page 255
- [show ip route profile](#), on page 256
- [show ip route summary](#), on page 258
- [show ip route supernets-only](#), on page 260
- [show ip route tag](#), on page 261
- [show ip route track-table](#), on page 264
- [show ip static route](#), on page 265
- [show ip static route bfd](#), on page 266
- [show ip route vrf](#), on page 268
- [show ipv6 policy](#), on page 275
- [show ipv6 route](#), on page 276
- [show ipv6 route shortcut](#), on page 281
- [show ipv6 route summary](#), on page 283
- [show ipv6 route tag](#), on page 285
- [show ipv6 route vrf](#), on page 287
- [show isis fast-reroute](#), on page 290
- [show key chain](#), on page 292
- [show monitor event-trace](#), on page 293
- [show platform hardware qfp active feature cef-mpls prefix ip](#), on page 299
- [show platform hardware qfp active feature cef-mpls prefix ipv6](#), on page 301
- [show platform hardware qfp active feature cef-mpls prefix mpls](#), on page 303
- [show platform software ip fp active cloudsec](#) , on page 305
- [show platform software ip rp active cloudsec](#) , on page 306
- [show route-map](#), on page 307
- [show route-tag list](#), on page 312
- [traffic-share min](#), on page 314
- [vccv](#), on page 315
- [vccv bfd status signaling](#), on page 317
- [vccv bfd template](#), on page 319

## 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 {infiniteend-time | duration seconds}
no send-lifetime start-time {infiniteend-time | duration seconds}
```

Syntax Description	
<i>start-time</i>	Beginning time that the key specified by the <b>key</b> command is valid to be sent. The syntax can be either of the following:  <i>hh</i> : <i>mm</i> : <i>ss</i> <i>Month</i> <i>date</i> <i>year</i> <i>hh</i> : <i>mm</i> : <i>ss</i> <i>date</i> <i>Month</i> <i>year</i> <ul style="list-style-type: none"> <li>• <i>hh</i> --hours</li> <li>• <i>mm</i> --minutes</li> <li>• <i>ss</i> -- seconds</li> <li>• <i>Month</i> -- first three letters of the month</li> <li>• <i>date</i> -- date (1-31)</li> <li>• <i>year</i>-- year (four digits)</li> </ul> <p>The default start time and the earliest acceptable date is January 1, 1993.</p>
<b>infinite</b>	Key is valid to be sent from the <i>start-time</i> value on.
<i>end-time</i>	Key is valid to be sent from the <i>start-time</i> value until the <i>end-time</i> value. The syntax is the same as that for the <i>start-time</i> value. The <i>end-time</i> value must be after the <i>start-time</i> value. The default end time is an infinite time period.
<b>duration</b> <i>seconds</i>	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.

**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**

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

# send-id

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

**send-id** *ID*

## Syntax Description

<i>ID</i>	Specifies the receive identifier. An integer between 0 to 255.
-----------	--

## Command Default

No key chain exists.

## Command Modes

Key chain key configuration (config-keychain-key)

## Command History

Release	Modification
16.12.1	This command was introduced.

## Usage Guidelines

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

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

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

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

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

## Related Commands

Command	Description
<b>accept-lifetime</b>	Sets the time period during which the authentication key on a key chain is received as valid.
<b>ip rip authentication key-chain</b>	Enables authentication for RIP Version 2 packets and specifies the set of keys that can be used on an interface.
<b>ip authentication key-chain eigrp</b>	Enables authentication of EIGRP packets.
<b>key</b>	Identifies an authentication key on a key chain.
<b>key chain</b> <i>key-name</i> <b>tcp</b>	Defines a TCP-AO authentication key-chain needed to enable authentication for routing protocols.
<b>key-string</b> (authentication)	Specifies the authentication string for a key.



Command	Description
<b>send-lifetime</b>	Sets the time period during which an authentication key on a key chain is valid to be sent.
<b>show key chain</b>	Displays authentication key information.

## set automatic-tag

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

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

### Examples

The following example configures the Cisco 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
<b>match as-path</b>	Matches a BGP autonomous system path access list.
<b>match community</b>	Matches a BGP community.

Command	Description
<b>match interface (IP)</b>	Distributes any routes that have their next hop out one of the interfaces specified.
<b>match ip address</b>	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.
<b>match ip next-hop</b>	Redistributes any routes that have a next hop router address passed by one of the access lists specified.
<b>match ip route-source</b>	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
<b>match metric (IP)</b>	Redistributes routes with the metric specified.
<b>match route-type (IP)</b>	Redistributes routes of the specified type.
<b>match tag</b>	Redistributes routes in the routing table that match the specified tags.
<b>route-map (IP)</b>	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
<b>set as-path</b>	Modifies an autonomous system path for BGP routes.
<b>set community</b>	Sets the BGP communities attribute.
<b>set level (IP)</b>	Indicates where to import routes.
<b>set local-preference</b>	Specifies a preference value for the autonomous system path.
<b>set metric (BGP, OSPF, RIP)</b>	Sets the metric value for a routing protocol.
<b>set metric-type</b>	Sets the metric type for the destination routing protocol.
<b>set next-hop</b>	Specifies the address of the next hop.
<b>set tag (IP)</b>	Sets a tag value of the destination routing protocol.
<b>set weight</b>	Specifies the BGP weight for the routing table.
<b>show route-map</b>	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 **set default interface** 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		
	<i>type</i>	Interface type, used with the interface number, to which packets are output.
	<i>number</i>	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 (config-route-map)

Command History	Release	Modification
	11.0	This command was introduced.
	12.3(7)T	This command was modified. This command was updated for use in configuring IPv6 policy-based routing (PBR).
	12.2(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 integrated into Cisco IOS XE Release 3.2S.
	15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

**Usage Guidelines** 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 Cisco software has no explicit route for the destination, then it routes the packet to this interface. The first interface specified with the **set default interface** command is used. The optionally specified interfaces 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 **ip policy route-map** command identifies a route map by name. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the match criteria—the conditions under which policy routing occurs. The **set** commands specify the set actions—the particular routing actions to perform if the criteria enforced by the **match** commands are met.

In PBR for IPv6, use the **ipv6 policy route-map** or **ipv6 local policyroute-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**

## 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
<b>ip policy route-map</b>	Identifies a route map to use for policy routing on an interface.
<b>ipv6 local policy route-map</b>	Identifies a route map to use for local IPv6 PBR.
<b>ipv6 policy route-map</b>	Configures IPv6 PBR on an interface.
<b>match ip address</b>	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.
<b>match ipv6 address</b>	Distributes IPv6 routes that have a prefix permitted by a prefix list or specifies an IPv6 access list to use to match packets for PBR for IPv6.
<b>match length</b>	Bases policy routing on the Level 3 length of a packet.
<b>route-map</b>	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
<b>set default interface</b>	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.
<b>set interface</b>	Indicates where to output packets that pass a match clause of route map for policy routing.
<b>set ip default next-hop verify-availability</b>	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.
<b>set ipv6 default next-hop</b>	Specifies an IPv6 default next hop to which matching packets will be forwarded.

Command	Description
<b>set ip next-hop</b>	Indicates where to output packets that pass a match clause of a route map for policy routing.
<b>set ipv6 next-hop (PBR)</b>	Indicates where to output IPv6 packets that pass a match clause of a route map for policy routing.
<b>set ipv6 precedence</b>	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 **set interface** 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

<i>type</i>	Interface type, used with the interface number, to which packets are forwarded.
<i>number</i>	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 modified. 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 integrated into Cisco IOS XE Release 3.2S.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

### Usage Guidelines

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

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

In PBR for IPv6, use the **ipv6 policy route-map** or **ipv6 local policy route-map** command with **match** and **set** route-map configuration commands to define conditions for policy-routing packets.

If the first interface specified with the **set interface** 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 **set interface null 0** 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 **set interface** command in a policy, the packets are processed in the hardware. In previous releases, PBR packets sent over TE tunnels are fast switched by Route Processor software.

## 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
```

The following example for IPv6 shows that 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 **set interface** 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 pl
 !
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
	<b>ip policy route-map</b>	Identifies a route map to use for policy routing on an interface.
	<b>ipv6 local policy route-map</b>	Configures PBR for IPv6 for originated packets.
	<b>ipv6 policy route-map</b>	Configures IPv6 PBR on an interface.
	<b>match ip address</b>	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.
	<b>match ipv6 address</b>	Specifies an IPv6 access list to use to match packets for PBR for IPv6.
	<b>match length</b>	Bases policy routing on the Level 3 length of a packet.
	<b>route-map</b>	Defines the conditions for redistributing routes from one routing protocol into another or enables policy routing.
	<b>set default interface</b>	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.
	<b>set ip default next-hop verify-availability</b>	Indicates where to forward packets that pass a match clause of a route map for policy routing and for which the Cisco software has no explicit route to a destination.
	<b>set ip next-hop</b>	Indicates where to forward packets that pass a match clause of a route map for policy routing.
	<b>set ipv6 default next-hop</b>	Specifies an IPv6 default next hop to which matching packets will be forwarded.
	<b>set ipv6 next-hop (PBR)</b>	Indicates where to output IPv6 packets that pass a match clause of a route map for policy routing.
	<b>set ipv6 precedence</b>	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 **set ip default next-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]
```

<b>Syntax Description</b>	<i>ip-address</i>	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

<b>Command History</b>	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 **set ip default next-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 **ip policy route-map** command identifies a route map by name. Each **route-map** command has a list of match and set commands associated with it. The match commands specify the *match criteria*--the conditions under which policy routing occurs. The **set** commands specify the *set actions*--the particular routing actions to perform if the criteria enforced by the **match** commands are met.

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.

### 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
<b>ip policy route-map</b>	Identifies a route map to use for policy routing on an interface.
<b>match ip address</b>	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.
<b>match length</b>	Bases policy routing on the Level 3 length of a packet.
<b>route-map (IP)</b>	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
<b>set default interface</b>	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.
<b>set interface</b>	Indicates where to output packets that pass a match clause of route map for policy routing.
<b>set ip next-hop</b>	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 command**  
**set 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 null routed if the configured next hop becomes unavailable.

**Examples** The following example:

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

Related Commands	Command	Description
	<b>set ip default next-hop verify-availability</b>	Configures policy routing to verify if the next hops of a route map are CDP neighbors before policy routing to those next hops.
	<b>set ip next-hop</b>	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 **set ip global** 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]
```

<b>Syntax Description</b>	<b>next-hop</b> <i>ip-address</i>	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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	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.

## 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
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>ip policy route-map</b>	Identifies a route map to use for policy routing on an interface.
	<b>match ip address</b>	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.
	<b>match length</b>	Bases policy routing on the Level 3 length of a packet.
	<b>route-map (IP)</b>	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
	<b>set default interface</b>	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
<b>set interface</b>	Indicates where to output packets that pass a match clause of a route map for policy routing.
<b>set ip default next-hop</b>	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.
<b>set ip vrf</b>	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 **set ip next-hop** command in route-map configuration mode. To delete an entry indicating where to output the packets, 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]} | dynamic dhcp | encapsulate l3vpn profile-name
| peer-address | recursive [{global | vrf vrf-name}] ip-address | verify-availability [{ip-address sequence
track track-object-number}]
```

### Catalyst 3850 Switches

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

#### Syntax Description

<i>ip-address</i>	IP address of the next hop to which packets are output. It must be the address of an adjacent router.
<b>dynamic dhcp</b>	Dynamically sets the DHCP next hop.
<b>encapsulate l3vpn</b>	Sets the encapsulation profile for the L3VPN next hop.
<i>profile-name</i>	L3VPN encapsulation profile name.
<b>peer-address</b>	Sets the next hop as the Border Gateway Protocol peering address.
<b>recursive</b> <i>ip-address</i>	Sets the IP address of the recursive next-hop router. <b>Note</b> The next-hop IP address must be assigned separately from the recursive next-hop IP address.
<b>global</b>	(Optional) Sets the global routing table.
<b>vrf</b> <i>vrf-name</i>	(Optional) Sets the Virtual Routing and Forwarding instance.
<b>verify-availability</b>	Verifies if the next hop is reachable.
<i>sequence</i>	(Optional) The sequence to be inserted into the next-hop list. The range is from 1 to 65535.
<b>track</b>	(Optional) Sets the next hop depending on the state of a tracked object.
<i>track-object-number</i>	(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	This command was modified. The <b>recursive</b> 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 integrated into the Cisco ASR 1000 Series Routers.
12.2(33)SRE	This command was modified. The <b>encapsulate</b> and <b>l3vpn</b> keywords were added.
Cisco IOS XE 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE. The <b>set ip next-hop ip-address [...ip-address]</b> command is available on Catalyst 3850 Series switches.

## Usage Guidelines

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

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 conditions for policy routing packets. The **ip policy route-map** command identifies a route map by name. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*--the conditions under which policy routing occurs. The **set** commands specify the *set actions*--particular routing actions to be performed if the criteria enforced by the **match** commands are met.

If the interface associated with the first next hop, which is specified with the **set ip next-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 the **set ip default next-hop** commands are similar but have a different order of operations. Configuring the **set ip next-hop** command causes the system to use policy-based 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 the policy route to the specified next hop.





**Note** The **set ip next-hop** command does not support Inherit-VRF routing on Cisco 7600 series routers because the **set ip next-hop ip-address** command is treated as equivalent to the **set ip global next-hop ip-address** command on Cisco 7600 series routers. (Inherit-VRF routing enables packets arriving on a VRF interface to be routed by the same outgoing interface.) Therefore, when using Cisco 7600 series routers, we recommend that you use the **set ip vrf vrf next-hop** command to explicitly indicate the VRF from which the next hop is to be chosen. We also recommend that in Cisco 7600 series routers, the **set ip next-hop** command be used only for route maps applied on non-VRF interfaces, where the software behavior and the hardware behavior would be similar.

## Examples

The following example shows how 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
```

The following example shows how IP address 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
<b>ip policy route-map</b>	Identifies a route map to use for policy routing on an interface.
<b>match ip address</b>	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.
<b>match length</b>	Bases policy routing on the Level 3 length of a packet.
<b>route-map (IP)</b>	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
<b>set default interface</b>	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.
<b>set interface</b>	Indicates where to output packets that pass a match clause of a route map for policy routing.
<b>set ip default next-hop verify-availability</b>	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

<i>next-hop-address</i>	(Optional) IP address of the next hop to which packets will be forwarded.
<i>sequence</i>	(Optional) Sequence of next hops. The acceptable range is from 1 to 65535.
<b>track</b>	(Optional) The tracking method is track.
<i>object</i>	(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 <b>track</b> keyword and <i>next-hop-address</i> , <i>sequence</i> , and <i>object</i> arguments were added.
12.3(14)T	The SAA feature (uses <b>rtr</b> commands) was replaced by the IP SLAs feature (uses <b>ipsla</b> commands).
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.

### 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.

---

## Examples

The following configuration sample demonstrates the use of 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. 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
```

## Using Object Tracking

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**

<b>Command</b>	<b>Description</b>
<b>show route-map</b>	Displays the configured route maps.
<b>show track</b>	Displays information about objects that are tracked by the tracking process.
<b>track</b>	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

<i>vrf-name</i>	Name of the VRF.
<b>next - hop</b> <i>ip-address</i>	IP address of the next hop to which packets are forwarded. The next hop must be an adjacent router.
<b>next - hop recursive</b> <i>ip-address</i>	IP address of the recursive next-hop router. <b>Note</b> 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

### 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
<b>ip policy route-map</b>	Identifies a route map to use for policy routing on an interface.
<b>match ip address</b>	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.
<b>match length</b>	Bases policy routing on the Level 3 length of a packet.
<b>route-map</b>	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
<b>set default interface</b>	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.
<b>set interface</b>	Indicates where to output packets that pass a match clause of a route map for policy routing.
<b>set ip default next-hop</b>	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.
<b>set ip next-hop</b>	Indicates where to output packets that pass a match clause of a route map for policy routing.

## set ipv6 default next-hop

To specify an IPv6 default next hop to which matching packets are forwarded, use the **set ipv6 default next-hop** command in route-map configuration mode. To delete the default next hop, use the **no** form of this command.

```
set ipv6 default [{vrf vrf-name | global}] next-hop global-ipv6-address [global-ipv6-address...]
no set ipv6 default [{vrf vrf-name | global}] next-hop global-ipv6-address [global-ipv6-address...]
```

### Syntax Description

<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies explicitly that the default next-hops are under the specific Virtual Routing and Forwarding (VRF) instance.
<b>global</b>	(Optional) Specifies explicitly that the default next-hops are under the global routing table.
<i>global-ipv6-address</i>	IPv6 global address of the next hop to which packets are output. The next-hop router must be an adjacent router.  This argument must be in the form documented in RFC 2373, where the address is specified in hexadecimal using 16-bit values between colons.

### Command Default

Packets are not forwarded to a default next hop.

### Command Modes

Route-map configuration (config-route-map)

### Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)S.
12.2(33)SX14	This command was integrated into Cisco IOS Release 12.2(33)SX14.
Cisco IOS XE Release 3.2S	This command was modified. It was integrated into Cisco IOS XE Release 3.2S.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

### Usage Guidelines

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *global-ipv6-address* argument.

Use the **set ipv6 default next-hop** command in policy-based routing PBR for IPv6 to specify an IPv6 next-hop address to which a packet is policy routed when the router has no route in the IPv6 routing table or the packets match the default route. The IPv6 next-hop address must be adjacent to the router; that is, reachable by using a directly connected IPv6 route in the IPv6 routing table. The IPv6 next-hop address also must be a global IPv6 address. An IPv6 link-local address cannot be used because the use of an IPv6 link-local address requires interface context.

If the software has no explicit route for the destination in the packet, then the software routes the packet to the next hop as specified by the **set ipv6 default next-hop** command. The optional specified IPv6 addresses are tried in turn.



Use the **ipv6 policy route-map** command, the **route-map** command, and the **match** and **set route-map** commands to define the conditions for PBR packets. The **ipv6 policy route-map** command identifies a route map by name. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the match criteria, which are the conditions under which PBR occurs. The **set** commands specify the set actions, which are 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 ipv6 next-hop**
2. **set interface**
3. **set ipv6 default next-hop**
4. **set default interface**



**Note** The **set ipv6 next-hop** and **set ipv6 default next-hop** are similar commands. The **set ipv6 next-hop** command is used to policy route packets for which the router has a route in the IPv6 routing table. The **set ipv6 default next-hop** command is used to policy route packets for which the router does not have a route in the IPv6 routing table (or the packets match the default route).

## Examples

The following example shows how to set the next hop to which the packet is routed:

```
ipv6 access-list match-dst-1
 permit ipv6 any 2001:DB8:4:1::1/64 any
route-map pbr-v6-default
 match ipv6 address match-dst-1
 set ipv6 default next-hop 2001:DB8:4:4::1/64
```

## Related Commands

Command	Description
<b>ipv6 local policy route-map</b>	Identifies a route map to use for local IPv6 PBR.
<b>ipv6 policy route-map</b>	Configures IPv6 policy-based routing (PBR) on an interface.
<b>match ipv6 address</b>	Specifies an IPv6 access list to use to match packets for PBR for IPv6.
<b>match length</b>	Bases policy routing on the Level 3 length of a packet.
<b>route-map (IP)</b>	Defines the conditions for redistributing routes from one routing protocol into another, or to enable policy routing.
<b>set default interface</b>	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.
<b>set interface</b>	Indicates where to output packets that pass a match clause of a route map for policy routing.
<b>set ipv6 next-hop (PBR)</b>	Indicates where to output IPv6 packets that pass a match clause of a route map for policy routing.

Command	Description
set ipv6 precedence	Sets the precedence value in the IPv6 packet header.

## set ipv6 next-hop (PBR)

To indicate where to output IPv6 packets that pass a match clause of a route map for policy-based routing (PBR), use the **set ipv6 next-hop** command in route-map configuration mode. To delete an entry, use the **no** form of this command.

```
set ipv6 next-hop {next-hop-ipv6-address [{next-hop-ipv6-address...}] | encapsulate l3vpn
encapsulation-profile | peer-address | recursive next-hop-ipv6-address | verify-availability
next-hop-ipv6-address sequence track object-number}
no set ipv6 next-hop {next-hop-ipv6-address [{next-hop-ipv6-address...}] | encapsulate l3vpn
encapsulation-profile | peer-address | recursive next-hop-ipv6-address | verify-availability
next-hop-ipv6-address sequence track object-number}
```

Syntax Description		
<i>next-hop-ipv6-address</i> [ <i>next-hop-ipv6-address ...</i> ]	IPv6 global address of the next hop to which packets are sent. The next-hop router must be an adjacent router.  The IPv6 address must be specified in hexadecimal using 16-bit values between colons as specified in RFC 2373.	
<b>encapsulate</b>	Specifies the encapsulation profile for the next-hop VPN.	
<b>l3vpn</b>	Specifies Layer 3 VPN encapsulation.	
<i>encapsulation-profile</i>	Encapsulation profile name.	
<b>peer-address</b>	Specifies the peer address. This keyword is specific to Border Gateway Protocol (BGP).	
<b>recursive</b> <i>next-hop-ipv6-address</i>	Specifies the IPv6 address of the recursive next-hop router. <ul style="list-style-type: none"> <li>The next-hop IPv6 address must be assigned separately from the recursive next-hop IPv6 address.</li> </ul>	
<b>verify-availability</b>	Verifies if the next-hop router is reachable.	
<i>sequence</i>	Sequence number to insert into the next-hop list. Valid values for the <i>sequence</i> argument are from 1 to 65535.	
<b>track</b> <i>object-number</i>	Sets the next-hop router depending on the state of a tracked object number. Valid values for the <i>object-number</i> argument are from 1 to 1000.	

**Command Default** Packets are not forwarded to a default next hop.

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

Command History	Release	Modification
	12.3(7)T	This command was introduced.
	12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)S.

Release	Modification
12.2(33)SX14	This command was integrated into Cisco IOS Release 12.2(33)SX14.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
15.4(2)S	This command was modified. The <b>recursive</b> keyword was added.

### Usage Guidelines

The **set ipv6 next-hop** command is similar to the **set ip next-hop** command, except that it is IPv6-specific. An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *next-hop-ipv6-address* argument. You must specify an IPv6 address; an IPv6 link-local address cannot be used because the use of an IPv6 link-local address requires interface context.

The *next-hop-ipv6-address* argument must specify an address that is configured in the IPv6 Routing Information Base (RIB) and is directly connected. A directly connected address is covered by an IPv6 prefix configured on an interface, or an address covered by an IPv6 prefix specified on a directly connected static route.

### Examples

The following example shows how to set the next hop to which packets are routed:

```
ipv6 access-list match-dst-1
  permit ipv6 any 2001:DB8::1 any
!
route-map pbr-v6-default
  match ipv6 address match-dst-1
  set ipv6 next-hop 2001:DB8::F
```

### Related Commands

Command	Description
<b>ipv6 local policy route-map</b>	Identifies a route map to use for local IPv6 PBR.
<b>ipv6 policy route-map</b>	Configures IPv6 PBR on an interface.
<b>match ipv6 address</b>	Specifies an IPv6 access list to use to match packets for PBR for IPv6.
<b>match length</b>	Bases policy routing on the Level 3 length of a packet.
<b>route-map (IP)</b>	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
<b>set default interface</b>	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.
<b>set interface</b>	Indicates where to output packets that pass a match clause of a route map for policy routing.
<b>set ipv6 default next-hop</b>	Specifies an IPv6 default next hop to which matching packets are forwarded.
<b>set ipv6 precedence</b>	Sets the precedence value in the IPv6 packet header.

# set ipv6 precedence

To set the precedence value in the IPv6 packet header, use the **set ipv6 precedence** command in route-map configuration mode. To remove the precedence value, use the **no** form of this command.

**set ipv6 precedence** *precedence-value*  
**no set ipv6 precedence** *precedence-value*

## Syntax Description

<i>precedence-value</i>	A number from 0 to 7 that sets the precedence bit in the packet header.
-------------------------	---

## Command Modes

Route-map configuration (config-route-map)

## Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)S.
12.2(33)SX14	This command was integrated into Cisco IOS Release 12.2(33)SX14.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

## Usage Guidelines

The way the network gives priority (or some type of expedited handling) to the marked traffic is through the application of weighted fair queueing (WFQ) or weighted random early detection (WRED) at points downstream in the network. Typically, you would set IPv6 precedence at the edge of the network (or administrative domain) and have queueing act on it thereafter. WFQ can speed up handling for high precedence traffic at congestion points. WRED ensures that high precedence traffic has lower loss rates than other traffic during times of congestion.

The mapping from keywords such as routine and priority to a precedence value is useful only in some instances. That is, the use of the precedence bit is evolving. You can define the meaning of a precedence value by enabling other features that use the value. In the case of Cisco high-end Internet quality of service (QoS), IPv6 precedences can be used to establish classes of service that do not necessarily correspond numerically to better or worse handling in the network. For example, IPv6 precedence 2 can be given 90 percent of the bandwidth on output links in the network, and IPv6 precedence 6 can be given 5 percent using the distributed weight fair queueing (DWFQ) implementation on the Versatile Interface Processors (VIPs).

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, or for policy routing. 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 or policy routing is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular redistribution or policy routing actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **set route-map** configuration commands specify the redistribution set actions 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.

**Examples**

The following example sets the IPv6 precedence value to 5 for packets that pass the route map match:

```
interface serial 0
  ipv6 policy route-map texas
!
route-map cisco1
  match length 68 128
  set ipv6 precedence 5
```

**Related Commands**

Command	Description
<b>ipv6 local policy route-map</b>	Identifies a route map to use for local IPv6 PBR.
<b>ipv6 policy route-map</b>	Configures IPv6 PBR on an interface.
<b>match ipv6 address</b>	Specifies an IPv6 access list to use to match packets for PBR for IPv6.
<b>match length</b>	Bases policy routing on the Level 3 length of a packet.
<b>route-map (IP)</b>	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
<b>set default interface</b>	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.
<b>set interface</b>	Indicates where to output packets that pass a match clause of a route map for policy routing.
<b>set ipv6 default next-hop</b>	Specifies an IPv6 default next hop to which matching packets will be forwarded.
<b>set ipv6 next-hop</b>	Indicates where to output IPv6 packets that pass a match clause of a route map for policy routing.
<b>set ipv6 precedence</b>	Sets the precedence value in the IPv6 packet header.

## set level (IP)

To indicate where to import routes, use the **set level** 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-area** and **backbone** keywords have no effect on where routes are imported.

### Examples

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

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

**Related Commands**

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



# set local-preference

To specify a preference value for the autonomous system paths that pass the route map, use the **set local-preference** command in route-map configuration mode. To delete the entry from the route map, use the **no set local-preference** form of this command.

**set local-preference** *number*  
**no set local-preference**

<b>Syntax Description</b>	<i>number</i> Preference value. An integer from 0 to 4294967295.
---------------------------	--

**Command Default** Preference value of 100

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	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 local preference attribute is a number that indicates the relative preference of one route over another when there is more than one route to a destination. A higher preference causes a route to be preferred over a route with a lower preference.

This attribute is exchanged between iBGP peers only. That is, the preference is sent to all routers in the local autonomous system only. This attribute is used to determine local policy

You can change the default preference value with the **bgp default local-preference** command.

## Examples

The following example sets the local preference to 200 for all routes that are included in access list 1:

```
route-map map-preference
 match as-path 1
 set local-preference 200
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>bgp default local-preference</b>	Changes the default local preference value.
	<b>match as-path</b>	Matches a BGP autonomous system path access list.
	<b>match community</b>	Matches a BGP community.

Command	Description
<b>match interface (IP)</b>	Distributes routes that have their next hop out one of the interfaces specified.
<b>match ip address</b>	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.
<b>match ip next-hop</b>	Redistributes any routes that have a next hop router address passed by one of the access lists specified.
<b>match ip route-source</b>	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
<b>match metric (IP)</b>	Redistributes routes with the metric specified.
<b>match route-type (IP)</b>	Redistributes routes of the specified type.
<b>match tag</b>	Redistributes routes in the routing table that match the specified tags.
<b>route-map (IP)</b>	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
<b>set automatic-tag</b>	Automatically computes the tag value.
<b>set community</b>	Sets the BGP communities attribute.
<b>set ip next-hop</b>	Specifies the address of the next hop.
<b>set level (IP)</b>	Indicates where to import routes.
<b>set metric (BGP, OSPF, RIP)</b>	Sets the metric value for a routing protocol.
<b>set metric-type</b>	Sets the metric type for the destination routing protocol.
<b>set origin (BGP)</b>	Sets the BGP origin code.
<b>set tag (IP)</b>	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*

<b>Syntax Description</b>	<i>metric-value</i>	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)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	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.

### Examples

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

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

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>match as-path</b>	Matches a BGP autonomous system path access list.
	<b>match community</b>	Matches a BGP community.

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

## set metric-type

To set the metric type for the destination routing protocol, use the **set metric-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).

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

# set next-hop

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

**set next-hop command** **set next-hop** *next-hop*  
**no set next-hop** *next-hop*

## Syntax Description

<i>next-hop</i>	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 *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 **route-map** command deletes the route map.

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

## 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
<b>match as-path</b>	Matches a BGP autonomous system path access list.
<b>match community</b>	Matches a BGP community.
<b>match interface (IP)</b>	Distributes routes that have their next hop out one of the interfaces specified.

Command	Description
<b>match ip address</b>	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.
<b>match ip next-hop</b>	Redistributes any routes that have a next hop router address passed by one of the access lists specified.
<b>match ip route-source</b>	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
<b>match metric (IP)</b>	Redistributes routes with the metric specified.
<b>match route-type (IP)</b>	Redistributes routes of the specified type.
<b>match tag</b>	Redistributes routes in the routing table that match the specified tags.
<b>route-map (IP)</b>	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
<b>set automatic-tag</b>	Automatically computes the tag value.
<b>set community</b>	Sets the BGP communities attribute.
<b>set ip next-hop</b>	Specifies the address of the next hop.
<b>set level (IP)</b>	Indicates where to import routes.
<b>set local-preference</b>	Specifies a preference value for the autonomous system path.
<b>set metric (BGP, OSPF, RIP)</b>	Sets the metric value for a routing protocol.
<b>set metric-type</b>	Sets the metric type for the destination routing protocol.
<b>set origin (BGP)</b>	Sets the BGP origin code.
<b>set tag (IP)</b>	Sets the value of the destination routing protocol.
<b>set weight</b>	Specifies the BGP weight for the routing table.



## set tag (IP)

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

```
set tag {tag-value|tag-value-dotted-decimal}
no set tag {tag-value|tag-value-dotted-decimal}
```

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

**Command Default** Routes are not tagged.

**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.
	15.2(2)S	This command was modified. This command was integrated into Cisco IOS Release 15.2(2)S and the <i>tag-value-dotted-decimal</i> argument was added to support tag values in dotted-decimal format.
	Cisco IOS XE Release 3.6S	This command was modified. The <i>tag-value-dotted-decimal</i> argument was added to support tag values in dotted-decimal format.

**Usage Guidelines** Use the **set tag** command to set an administrative tag for a route within a route map. Route tags are 32-bit values attached to routes. You can set tag values as plain decimals or dotted decimals. Route tags are used by route maps to filter routes. The tag value has no impact on routing decisions. It is used to mark or flag routes to prevent routing loops when routes are redistributed between routing protocols.

### Examples

The following example shows how to set the tag value of the destination routing protocol to 5:

```
Device(config)# route-map tag
Device(config-route-map)# set tag 5
```

The following example shows how to set the tag value in the dotted-decimal format:

```
Device(config)# route-map tag  
Device(config-route-map)# set tag 10.10.10.10
```

**Related Commands**

Command	Description
<b>match tag</b>	Filters routes that match specific route tags.
<b>route-map (IP)</b>	Defines conditions for redistributing routes from one routing protocol into another, or enables policy routing.
<b>set automatic-tag</b>	Automatically computes the tag value.

## set vrf next-hop verify-availability

To configure policy routing to verify the reachability of the next hop of a route map of a VRF instance before the device performs policy routing to that next hop, use the **set {ip | ipv6} vrf next-hop verify-availability** command in route-map configuration mode. To disable this function, use the **no** form of this command.

```
set {ip | ipv6} vrf vrf-name next-hop verify-availability next-hop-address sequence track object
no set {ip | ipv6} vrf vrf-name next-hop verify-availability next-hop-address sequence track object
```

Syntax Description		
	<i>vrf-name</i>	Name of the VRF instance.
	<i>next-hop-address</i>	IP address of the next hop to which packets will be forwarded.
	<i>sequence</i>	Sequence of next hops. The range is from 1 to 65535.
	<b>track</b>	Specifies the tracking method.
	<i>object</i>	Object number that the tracking subsystem is tracking. The range is from 1 to 1000.

**Command Default** The reachability of the next hop of a route map in a VRF instance before a device performs policy routing is not verified.

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

Command History	Release	Modification
	Cisco IOS XE Release 3.11S	This command was introduced.

**Usage Guidelines** Use the **set {ip | ipv6} vrf next-hop verify-availability** to support object tracking using Internet Control Message Protocol (ICMP) ping or an HTTP GET request to verify if a remote device is reachable. With optional arguments to support object tracking, this command allows policy based routing (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).

PBR informs 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 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.

### Example

The following example shows how to configure policy routing to verify the reachability of the next hop of a route map of a VRF instance:

```
Device> enable
Device# configure terminal
Device(config)# ip vrf RED
Device(config-vrf)# rd 100:1
Device(config-vrf)# route-target export 100:1
Device(config-vrf)# route-target import 100:1
Device(config-vrf)# exit
Device(config)# ip sla 1
Device(config-ip-sla)# icmp-echo 10.0.0.4
Device(config-ip-sla-echo)# vrf RED
Device(config-ip-sla-echo)# exit
Device(config)# ip sla schedule 1 life forever start-time now
Device(config)# track 1 ip sla 1
Device(config-track)# interface Ethernet0/0
Device(config-if)# ip vrf forwarding RED
Device(config-if)# ip address 10.0.0.2 255.0.0.0
Device(config-if)# exit
Device(config)# route-map test02 permit 10
Device(config-route-map)# set ip vrf RED next-hop verify-availability 192.168.23.2 1 track
Device(config-route-map)# interface Ethernet0/0
Device(config-if)# ip vrf forwarding RED
Device(config-if)# ip policy route-map test02
Device(config-if)# ip address 192.168.10.2 255.255.255.0
Device(config-if)# end
```

The following example shows how to configure policy routing to verify the reachability of the next hop of a route map of an IPv6 VRF instance:

```
Device> enable
Device# configure terminal
Device(config)# ip vrf RED
Device(config-vrf)# rd 100:1
Device(config-vrf)# route-target export 100:1
Device(config-vrf)# route-target import 100:1
Device(config-vrf)# exit
Device(config)# ip sla 1
Device(config-ip-sla)# icmp-echo 10.0.0.4
Device(config-ip-sla-echo)# vrf RED
Device(config-ip-sla-echo)# exit
Device(config)# ip sla schedule 1 life forever start-time now
Device(config)# track 1 ip sla 1
Device(config-track)# interface Ethernet0/0
Device(config-if)# ip vrf forwarding RED
Device(config-if)# ip policy route-map test02
Device(config-if)# ip address 192.168.10.2 255.255.255.0
```

```
Device(config-if)# ipv6 address 2001:DB8::/32
Device(config-if)# interface Ethernet1/0
Device(config-if)# ip vrf forwarding RED
Device(config-if)# ip address 10.0.0.2 255.0.0.0
Device(config-if)# ipv6 address 2001:DB8::/48
Device(config-if)# exit
Device(config)# route-map test02 permit 10
Device(config-route-map)# set ipv6 vrf RED next-hop verify-availability 2001:DB8:1::1 1
track 1
Device(config-route-map)# end
```

**Related Commands**

Command	Description
<b>show route-map</b>	Displays the configured route maps.
<b>track</b>	Tracks the state of an interface, an ip route, or a response time reporter.

# show bfd drops

To display the number of dropped packets in Bidirectional Forwarding Detection (BFD), use the **show bfd drops** 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.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.

## Examples

The following is sample output from the **show bfd drops** command. The IPV4 and IPV6 columns display single hop session counters for IPv4 and IPv6, respectively. The IPV4-M and IPV6-M columns display multihop session counters for IPv4 and IPv6, respectively.

```
Router# show bfd drops

BFD Drop Statistics

Invalid TTL          IPV4    IPV6    IPV4-M  IPV6-M  MPLS_PW  MPLS_TP_LSP
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 following is a sample output from **show bfd drops** command.

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

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

Field	Description
Invalid Header Bits	Some header bits are invalid or unexpected.
BFD Not Configured	A packet was received for a session that does not exist.

Field	Description
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
<b>show bfd neighbors</b>	Displays a line-by-line listing of existing BFD adjacencies
<b>show bfd summary</b>	Displays summary information for BFD.

# show bfd neighbors

To display a line-by-line listing of existing Bidirectional Forwarding Detection (BFD) adjacencies, use the **show bfd neighbors** 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

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

## Command Modes

User EXEC (>)

Privileged EXEC (#)

## Command History

S Release	Modification
12.0(31)S	This command was introduced.



<b>S Release</b>	<b>Modification</b>
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRC	This command was modified. The <b>vrf vrf-name</b> keyword and argument, the <b>client</b> keyword, and the <i>ip-address</i> 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 <b>details</b> keyword.
12.2(33)SRE	This command was modified. Support for IPv6 was added.
15.1(2)S	This command was modified. <ul style="list-style-type: none"> <li>• The <b>show bfd neighbors details</b> command output was changed for hardware-offloaded BFD sessions.</li> <li>• The <b>show bfd neighbors</b> command output was changed to display the header type to identify the session type.</li> </ul>
15.1(3)S	This command was modified to display information about multihop sessions.
15.2(4)S	This command was modified. The output of the command was enhanced to include Template and Authentication fields for single-hop sessions.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
15.4(3)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.
<b>T Release</b>	<b>Modification</b>
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.
15.1(2)T	This command was modified. Support for IPv6 was added.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
15.2(1)E	This command was integrated into Cisco IOS Release 15.2(1)E.
<b>XE Release</b>	<b>Modification</b>
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

**Usage Guidelines**

The **show bfd neighbors** 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 **show bfd neighbors** command with the **details** keyword on

the Cisco 12000 Series Internet Router, you must enter the command on the line card. Use the **attach slot** command to establish a CLI session with a line card.

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

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.

## Examples

The following is sample output from the **show bfd neighbors** that shows the status of the adjacency or neighbor:

```
Device# 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 is sample output from the **show bfd neighbors** command when it is entered with the **details** keyword that shows BFD protocol parameters and timers for each neighbor:

```
Device# 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 is sample output from the **show bfd neighbors** command when it is entered on a Cisco 12000 Series Internet Router Route Processor (RP) that shows the status of the adjacency or neighbor:

```
Device# 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 is sample output from the **show bfd neighbors** command when it is entered in a Cisco 12000 Series Internet Router RP that shows the status of the adjacency or neighbor with the **details** keyword:

```
Device# 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 is sample output from the **show bfd neighbors** command when it is entered on a Cisco 12000 Series Internet Router line card that shows the status of the adjacency or neighbor:

```

Device# attach 6

Entering Console for 8 Port Fast Ethernet in Slot: 6
Type "exit" to end this session
Press RETURN to get started!

Device> show bfd neighbors

Cleanup timer hits: 0
OurAddr      NeighAddr      LD/RD RH Holddown(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 is sample output from the **show bfd neighbors** command when it is entered on a Cisco 12000 Series Internet Router line card that shows the status of the adjacency or neighbor with the **details** keyword:

```

Device# attach 6

Entering Console for 8 Port Fast Ethernet in Slot: 6
Type "exit" to end this session
Press RETURN to get started!
Device> show bfd neighbors details

Cleanup timer hits: 0
OurAddr      NeighAddr      LD/RD RH Holddown(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
Holddown (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
Device>

```

## Examples

The following is sample output from the **show bfd neighbors details** command that shows that the BFD neighbor device is running BFD Version 1 and that the BFD session is up and running in echo mode:

## show bfd neighbors

Device# **show bfd neighbors details**

```

OurAddr      NeighAddr      LD/RD  RH/RS  Holddown(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
Holddown (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

```

The following is sample output from the **show bfd neighbors** command that displays all IPv6 sessions:

Device# **show bfd neighbors ipv6 2001::1**

```

OurAddr      NeighAddr      LD/RD  RH/RS  Holddown(mult)  State
Int
2001:DB8:0:ABCD::1  2001:DB8:0:ABCD::2  2/2    Up     0 (3)           Up
Et0/0
2001:DB8:0:1:FFFF:1234::5  2001:DB8:0:1:FFFF:1234::6  4/4    Up     0 (3)           Up
Et1/0

```

The following is a sample output from the **show bfd neighbors**

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

Device# **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
2001:DB8::1    9/0    Down   Down   Et0/0
2001:DB8:0:ABCD::1  10/0   Down   Down   Et0/0
2001:DB8::2    1/0    0 (RH) Fail   Et0/0
2001:DB8:0:1::1  2/0    Down   Down   Et0/0
2001:DB8:0:1:FFFF:1234::5  3/0    Down   Down   Et0/0

```

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

Device# **show bfd neighbors details**

```

IPv4 Sessions
NeighAddr      LD/RD  RH/RS  State  Int
100.0.2.1      127/156  Down   Init   Se0/5/1.1/2/1/1:0
Session Host: Hardware - session negotiated with platform adjusted timer values.
                MinTxInt - configured: 200000          adjusted: 1000000
OurAddr: 100.0.2.2
Handle: 2
Local Diag: 1, 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(0)
Rx Count: 5052
Tx Count: 7490
Elapsed time watermarks: 0 0 (last: 0)
Registered protocols: IPv4 Static CEF
Template: software
Downtime: 00:00:05
Last packet: Version: 1                - Diagnostic: 3
              State bit: Down          - Demand bit: 0
              Poll bit: 0              - Final bit: 0
              C bit: 1
              Multiplier: 3            - Length: 24
              My Discr.: 156          - Your Discr.: 0
              Min tx interval: 1000000 - Min rx interval: 1000000
              Min Echo interval: 200000

```

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 <b>show bfd neighbors details</b> command was entered.
NeighAddr	IPv4 or IPv6 address of the BFD adjacency or neighbor.
LD/RD	Local discriminator (LD) and remote discriminator (RD) being used for the session.
RH	Remote Heard (RH) Indicates that the remote BFD neighbor has been heard.
Holdown (mult)	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 <b>bfd</b> command.  <b>Note</b> BFD Version 1 and echo mode are supported only in Cisco IOS Release 12.4(9)T and later releases.
Rx Count	Number of BFD control packets that are received from the BFD neighbor.
Tx Count	Number of BFD control packets that are sent by the BFD neighbor.
Tx Interval	The interval, in milliseconds, between sent BFD packets.
Registered protocols	Routing protocols that are registered with BFD.

Field	Description
Last packet: Version:	<p>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. 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.</p> <p><b>Note</b> BFD Version 1 and echo mode are supported only in Cisco IOS Release 12.4(9)T and later releases.</p>
Diagnostic	<p>A diagnostic code specifying the local system's reason for the last transition of the session from Up to some other state.</p> <p>State values are as follows:</p> <ul style="list-style-type: none"> <li>• 0—No Diagnostic</li> <li>• 1—Control Detection Time Expired</li> <li>• 2—Echo Function Failed</li> <li>• 3—Neighbor Signaled Session Down</li> <li>• 4—Forwarding Plane Reset</li> <li>• 5—Path Down</li> <li>• 6—Concentrated Path Down</li> <li>• 7—Administratively Down</li> </ul>
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.
Poll bit	Indicates that the transmitting system is requesting verification of connectivity or verification of a parameter change.
Final bit	Indicates that the transmitting system is responding to a received BFD control packet that had a Poll (P) bit set.

Field	Description
Multiplier	<p>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.</p> <p>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, it indicates that a failure has occurred.</p> <p>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, it indicates that a failure has occurred.</p>
Length	Length of the BFD control packet, in bytes.
My Discr.	My Discriminator is a 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 is a discriminator that is 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.
Min Echo interval	<p>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.</p> <p>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.</p>

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.

Device# **show bfd neighbors details**

```

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

```

## show bfd neighbors

```

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

```

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

```

Device# 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:

```

Device# 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:

```

Device# 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
2001:DB8::1   1/1    Up     Up     Et0/0
2001:DB8:0:ABCD::1 2/2    Up     Up     Et0/0
2001:DB8::2   3/3    Up     Up     Et0/0
2001:DB8:0:1:FFFF:1234::5 4/4    Up     Up     Et0/0
2001:DB8:0:1::1 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 Multiprotocol Label Switching (MPLS) tunnel Transport Profile (TP) interface.
LSP type	Type of label-switched path for this session (Working or Protect).

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



```

Device# show bfd neighbors

IPv4 Sessions
NeighAddr          LD/RD          RH/RS          State          Int
192.0.2.6          1/12          Up             Up             Et0/0
Session state is UP and using echo function with 300 ms interval.
Session Host: Software
OurAddr: 192.0.2.12
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
Template: my-template
Authentication(Type/Keychain): sha-1/my-chain
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

```

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

**Table 5: show bfd neighbors Field Descriptions for Single-Hop BFD Sessions**

Field	Description
Template	BFD multihop template name.
Authentication	Authentication type and key chain.

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.

```

Device# show bfd neighbors

IPv4 Multihop Sessions
NeighAddr[vrf]          LD/RD          RH/RS          State
192.0.2.20             2/13          Up             Up
Session state is UP and not using echo function.
Session Host: Software
OurAddr: 192.0.2.21
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]: 192.0.2.1/24
  Source[vrf]: 192.0.2.2/24
  Template: mh
  Authentication(Type/Keychain): md5/qq

```

## show bfd neighbors

```

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 display.

**Table 6: show bfd neighbors Field Descriptions for Multihop BFD Sessions**

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

## Related Commands

Command	Description
<b>attach</b>	Connects to a specific line card to execute monitoring and maintenance commands on that line card.
<b>show bfd drops</b>	Displays the number of dropped packets in BFD.
<b>show bfd summary</b>	Displays summary information for BFD.

# show bfd summary

To display summary information for Bidirectional Forwarding Protocol (BFD), use the **show bfd summary** command in user EXEC or privileged EXEC mode.

**show bfd summary** [{client | session}]

Syntax Description	client	(Optional) Displays list of BFD clients and number of sessions created by each client.
	session	(Optional) Displays list of client-to-peer exchanges that have been launched by BFD clients, organized by session type.

## Command Modes

User EXEC (>)  
Privileged EXEC (#)

## Command History

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

## Usage Guidelines

Use this command to display summary information about BFD, BFD clients, or BFD sessions.

When a BFD client launches a session with a peer, BFD sends periodic BFD control packets to the peer. Information about the following states of a session are included in the output of this command:

- Up--When another BFD interface acknowledges the BFD control packets, the session moves into an up state.
- Down--The session, and data path, is declared down if a data path failure occurs and BFD does not receive a control packet within the configured amount of time. When a session is down, BFD notifies the BFD client so that the client can perform necessary actions to reroute traffic.

## Examples

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

```
Router# show bfd summary

Total                Session            Up            Down
                   1                1            0
```

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

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

```
Router# show bfd summary session

Protocol            Session            Up            Down
IPV4                 1                1            0
Total                1                1            0
```

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

## show bfd summary

```
Router# show bfd summary client
```

```
Client          Session      Up          Down
EIGRP           1            1           0
CEF             1            1           0
Total           2            2           0
```

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

**Table 7: show bfd summary Field Descriptions**

Field	Description
Session	Sum of launched sessions by type or when combined with Total, sum of all launched sessions.
Up	Number of sessions for which the BFD client acknowledged receipt of control packets.
Down	Number of sessions for which the BFD client did not receive control packets from a peer.
Total	Sum of all launched sessions, all Up sessions, or all Down sessions in list.
Protocol	Routing protocol of interface in a session.
Client	Type of client in a session.

---

**Related Commands**

Command	Description
<b>show bfd neighbors</b>	Displays list of existing BFD adjacencies.

# show dampening interface

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

**show dampening interface command** `show 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.

## Examples

The following is sample output from the **showdampeninginterface** 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 8: show dampening interface Field Descriptions**

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

**show dampening interface****Related Commands**

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

# show fm ipv6 pbr all

To display IPv6 policy-based routing (PBR) value mask results (VMRs), use the **show fm ipv6 pbr all** command in privileged EXEC mode.

**show fm ipv6 pbr all**

---

**Syntax Description**

This command has no arguments or keywords.

---

**Command Modes**

Privileged EXEC (#)

---

**Command History**

Release	Modification
12.2(33)SX14	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

---

**Usage Guidelines**

The **show fm ipv6 pbr all** command shows the IPv6 PBR VMRs for all interfaces on which IPv6 PBR is configured.

## show fm ipv6 pbr interface

To displays the IPv6 policy-based routing (PBR) value mask results (VMRs) on a specified interface, use the **show fm ipv6 pbr interface** command in privileged EXEC mode.

**show fm ipv6 pbr interface** *interface type number*

### Syntax Description

<b>interface</b> <i>type number</i>	Specified interface for which PBR VMR information will be displayed.
-------------------------------------	--

### Command Modes

Privileged EXEC (#)

### Command History

Release	Modification
12.2(33)SX14	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

### Usage Guidelines

The **show fm ipv6 pbr interface** command shows the IPv6 PBR VMRs for a specified interface.



# show interface dampening

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

**show interface dampening command** `show 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.

## Examples

The following is sample output from the **show interface dampening** 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 9: show interface dampening Field Descriptions**

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

**show interface dampening**

Field	Description
MaxP	Displays the maximum penalty.
Restart	Displays the restart timer.

**Related Commands**

Command	Description
<b>clear counters</b>	Clears the interface counters.
<b>dampening</b>	Enables IP event dampening at the interface level.
<b>show dampening interface</b>	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		
	<i>ip-prefix</i>	(Optional) IP address prefix of the entries to display.
	<i>mask</i>	(Optional) Subnet mask of the entries to display.
	<b>checksum</b>	(Optional) Displays FIB entry checksum information.
	<b>detail</b>	(Optional) Displays detailed FIB entry information.
	<b>internal checksum</b>	(Optional) Displays internal data structures. The <b>checksum</b> 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.

### 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
```

## show ip cef platform

```

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: 0005DC387B180003A011A57881000002884700012000

```

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

# show ip cache policy

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

**show 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.

## Examples

The following is sample output from the **show ip cache policy** 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 10: 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 <b>setipnext-hop</b> command. “Int” indicates the <b>setinterface</b> command.
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.

**show ip cache policy****Related Commands**

Command	Description
<b>ip route-cache</b>	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 **show ip local policy** command in EXEC mode.

**show ip local policy command** `show 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.

## Examples

The following is sample output from the **show ip local policy** 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 11: show ip local policy Field Descriptions**

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

## show ip local policy

Field	Description
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
<b>ip policy route-map</b>	Identifies a route map to use for local policy routing.
<b>match ip address</b>	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.
<b>match length</b>	Bases policy routing on the Level 3 length of a packet.
<b>route-map (IP)</b>	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
<b>set default interface</b>	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.
<b>set interface</b>	Indicates where to output packets that pass a match clause of route map for policy routing.
<b>set ip default next-hop verify-availability</b>	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.
<b>set ip next-hop</b>	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

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.

## 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 12: 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
<b>match ip address</b>	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.
<b>match length</b>	Bases policy routing on the Level 3 length of a packet.
<b>route-map (IP)</b>	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
<b>set default interface</b>	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.
<b>set interface</b>	Indicates where to output packets that pass a match clause of route map for policy routing.
<b>set ip default next-hop verify-availability</b>	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.
<b>set ip next-hop</b>	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 **show ip protocols** command in privileged EXEC mode.

**show ip protocols** command **show 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 **show ip protocols** command is useful in debugging routing operations. Information in the Routing Information Sources field of the **show ip protocols** output can help you identify a router suspected of delivering bad routing information.

Once you configure the **default-information originate on-passive** command, the output of the **show ip protocols** command displays that RIP default routes are sent on passive interfaces.

## Examples

The following sample output from the **show ip protocols** 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 13: 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 <b>distribute-listout</b> command.
Incoming update filter list for all interfaces...	Indicates whether a filter for incoming routing updates has been specified with the <b>distribute-listin</b> command.
Redistributing:	Indicates whether route redistribution has been enabled with the <b>redistribute</b> 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.
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 <b>auto-summary</b> command.
Routing for Networks:	Networks for which the routing process is currently injecting routes.

Field	Description
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: <ul style="list-style-type: none"> <li>• IP address</li> <li>• Administrative distance</li> <li>• Time the last update was received from this source</li> </ul>

### IS-IS Example

The following sample output from the **show ip protocols** 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 14: 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.

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: <ul style="list-style-type: none"> <li>• IP address</li> <li>• Administrative distance</li> <li>• Time the last update was received from this source</li> </ul>

### RIP Example

The following sample output from the **show ip protocols** 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 15: 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.
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: <ul style="list-style-type: none"> <li>• IP address</li> <li>• Administrative distance</li> <li>• Time the last update was received from this source</li> </ul>

### EIGRP NSF Awareness Verification Example

The following is sample output from the **show ip protocols** 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 16: 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.
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: <ul style="list-style-type: none"> <li>• IP address</li> <li>• Administrative distance</li> <li>• Time the last update was received from this source</li> </ul>

#### Related Commands

Command	Description
<b>auto-summary (EIGRP)</b>	Allows automatic summarization of subnet routes into network-level routes.
<b>default-information originate (RIP)</b>	Generates a default route into RIP.
<b>distribute-list in (IP)</b>	Filters networks received in updates.
<b>distribute-list out (IP)</b>	Suppresses networks from being advertised in updates.



Command	Description
<b>redistribute (IP)</b>	Redistributes routes from one routing domain into another routing domain.

## show ip route

To display contents of the routing table, use the **show ip route** 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

<i>ip-address</i>	(Optional) IP address for which routing information should be displayed.
<b>repair-paths</b>	(Optional) Displays the repair paths.
<b>next-hop-override</b>	(Optional) Displays the Next Hop Resolution Protocol (NHRP) next-hop overrides that are associated with a particular route and the corresponding default next hops.
<b>dhcp</b>	(Optional) Displays routes added by the Dynamic Host Configuration Protocol (DHCP) server.
<i>mask</i>	(Optional) Subnet mask.
<b>longer-prefixes</b>	(Optional) Displays output for longer prefix entries.
<i>protocol</i>	(Optional) The name of a routing protocol or the keyword <b>connected</b> , <b>mobile</b> , <b>static</b> , or <b>summary</b> . If you specify a routing protocol, use one of the following keywords: <b>bgp</b> , <b>eigrp</b> , <b>hello</b> , <b>isis</b> , <b>odr</b> , <b>ospf</b> , <b>nhrp</b> , or <b>rip</b> .
<i>process-id</i>	(Optional) Number used to identify a process of the specified protocol.
<b>list</b>	(Optional) Filters output by an access list name or number.
<i>access-list-number</i>	(Optional) Access list number.
<i>access-list-name</i>	(Optional) Access list name.
<b>static</b>	(Optional) Displays static routes.
<b>download</b>	(Optional) Displays routes installed using the authentication, authorization, and accounting (AAA) route download function. This keyword is used only when AAA is configured.
<b>update-queue</b>	(Optional) Displays Routing Information Base (RIB) queue updates.

### Command Modes

User EXEC (>)

Privileged EXEC (#)

### Command History

Release	Modification
9.2	This command was introduced.

Release	Modification
10.0	This command was modified. The “D—EIGRP, EX—EIGRP, N1—SPF NSSA external type 1 route” and “N2—OSPF NSSA external type 2 route” codes were included in the command output.
10.3	This command was modified. The <i>process-id</i> argument was added.
11.0	This command was modified. The <b>longer-prefixes</b> keyword was added.
11.1	This command was modified. The “U—per-user static route” code was included in the command output.
11.2	This command was modified. The “o—on-demand routing” code was included in the command output.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA, and the <b>update-queue</b> keyword was added.
11.3	This command was modified. The command output was enhanced to display the origin of an IP route in Intermediate System-to-Intermediate System (IS-IS) networks.
12.0(1)T	This command was modified. The “M—mobile” code was included in the command output.
12.0(3)T	This command was modified. The “P—periodic downloaded static route” code was included in the command output.
12.0(4)T	This command was modified. The “ia—IS-IS” code was included in the command output.
12.2(2)T	This command was modified. The command output was enhanced to display information on multipaths to the specified network.
12.2(13)T	This command was modified. The <i>egp</i> and <i>igrp</i> arguments were removed because the Exterior Gateway Protocol (EGP) and the Interior Gateway Routing Protocol (IGRP) were no longer available in Cisco software.
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	This command was modified. The command output was enhanced to display route tag information.
12.3(8)T	This command was modified. The command output was enhanced to display static routes using DHCP.

Release	Modification
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRE	This command was modified. The <b>dhcp</b> and <b>repair-paths</b> keywords were added.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5. The <b>next-hop-override</b> and <b>nhrp</b> keywords were added.
15.2(2)S	This command was modified. The command output was enhanced to display route tag values in dotted decimal format.
Cisco IOS XE Release 3.6S	This command was modified. The command output was enhanced to display route tag values in dotted decimal format.
15.2(4)S	This command was implemented on the Cisco 7200 series router.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
15.4(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

## Examples

The following is sample output from the **show ip route** command when an IP address is not specified:

```
Device# 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 sample output from the **show ip route** command includes routes learned from IS-IS Level 2:

```
Device# 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 10.0.0.0, 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 from the **show ip route ip-address mask longer-prefixes** command. When this keyword is included, the address-mask pair becomes the prefix, and any address that matches that prefix is displayed. Therefore, multiple addresses are displayed. 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 with 10.0.0.0. Any destinations that fall into that range are displayed in the output.

```
Device# 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 sample outputs from the **show ip route** command display all downloaded static routes. A “p” indicates that these routes were installed using the AAA route download function.

```
Device# 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 172.16.17.1 to network 10.0.0.0
```

```

       172.31.0.0/32 is subnetted, 1 subnets
P       172.31.229.41 is directly connected, Dialer1
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
```

```
Device# show ip route static
```

```

       172.16.4.0/8 is variably subnetted, 2 subnets, 2 masks
P       172.16.1.1/32 is directly connected, BRI0
P       172.16.4.0/8 [1/0] via 10.1.1.1, BRI0
S       172.31.0.0/16 [1/0] via 172.16.114.65, Ethernet0
S       10.0.0.0/8 is directly connected, BRI0
P       10.0.0.0/8 is directly connected, BRI0
       172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
S       172.16.114.201/32 is directly connected, BRI0
S       172.16.114.205/32 is directly connected, BRI0
S       172.16.114.174/32 is directly connected, BRI0
S       172.16.114.12/32 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 172.16.114.65, Ethernet0
S       172.16.0.0/16 [1/0] via 172.16.114.65, Ethernet0
```

The following sample output from the **show ip route static download** command displays all active and inactive routes installed using the AAA route download function:

```
Device# 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 remotel
I       10.38.1.9 255.255.255.0 192.168.69.1
```

The following sample outputs from the **show ip route nhrp** command display shortcut switching on the tunnel interface:

```
Device# 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
```

```
Device# show ip route nhrp
```

```
H       172.16.99.0 [250/1] via 10.1.1.99, 00:11:43, Tunnel0
```

The following are sample outputs from the **show ip route** command when the **next-hop-override** keyword is used. When this keyword is included, the NHRP next-hop overrides that are associated with a particular route and the corresponding default next hops are displayed.

```
=====
1) Initial configuration
=====
```

```
Device# 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
```

```
Device# 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
```

## show ip route

```

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

```

Device# **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
172.16.0.0/12	drop	
.		
.		
.		

2) Add a next-hop override

```

address = 10.10.10.0
mask = 255.255.255.0
gateway = 10.1.1.1
interface = Tunnel0

```

Device# **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

```

Device# **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

Device# 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 next-hop override
   address = 10.10.10.0
   mask = 255.255.255.0
   gateway = 10.11.1.1
   interface = Tunnel0
=====

Device# 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

Device# 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

```

## show ip route

```

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

```

Device# **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
.
.
.

```

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

**Table 17: show ip route Field Descriptions**

Field	Description
Codes (Protocol)	<p>Indicates the protocol that derived the route. It can be one of the following values:</p> <ul style="list-style-type: none"> <li>• B—BGP derived</li> <li>• C—Connected</li> <li>• D—Enhanced Interior Gateway Routing Protocol (EIGRP)</li> <li>• EX—EIGRP external</li> <li>• H—NHRP</li> <li>• i—IS-IS derived</li> <li>• ia—IS-IS</li> <li>• L—Local</li> <li>• M—Mobile</li> <li>• o—On-demand routing</li> <li>• O—Open Shortest Path First (OSPF) derived</li> <li>• P—Periodic downloaded static route</li> <li>• R—Routing Information Protocol (RIP) derived</li> <li>• S—Static</li> <li>• U—Per-user static route</li> <li>• +—Replicated route</li> </ul>

Field	Description
Codes (Type)	Type of route. It can be one of the following values: <ul style="list-style-type: none"> <li>• *—Indicates the last path used when a packet was forwarded. This information is specific to nonfast-switched packets.</li> <li>• E1—OSPF external type 1 route</li> <li>• E2—OSPF external type 2 route</li> <li>• IA—OSPF interarea route</li> <li>• L1—IS-IS Level 1 route</li> <li>• L2—IS-IS Level 2 route</li> <li>• N1—OSPF not-so-stubby area (NSSA) external type 1 route</li> <li>• N2—OSPF NSSA external type 2 route</li> </ul>
10.110.0.0	Indicates the address of the remote network.
[160/5]	The first number in brackets is the administrative distance of the information source; the second number is the metric for the route.
via 10.119.254.6	Specifies the address of the next device 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.

The following is sample output from the **show ip route** command when an IP address is specified:

```
Device# 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, the router includes one of its IP addresses to be used as the originator IP address. When other routers calculate IP routes, they store the originator IP address with each route in the routing table.

The preceding example shows the output from the **show ip route** 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 the origin of a particular IP route in your network. In the preceding example, the route to 10.0.0.1/32 was originated by a device with IP address 10.191.255.247.

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

**Table 18: 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.
Redistributing via...	Indicates the redistribution protocol.
Last update from 10.191.255.251	Indicates the IP address of the router that is the next hop to the remote network and the 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	Indicates the number of packets transmitted over various routes.

The following sample output from the **show ip route** command displays the tag applied to the route 10.22.0.0/16. You must specify an IP prefix to see the tag value. The fields in the display are self-explanatory.

```
Device# 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
```

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 172.16.2.2 [1/0] are static, and route 10.0.0.0/0 is a default route candidate. The fields in the display are self-explanatory.

```
Device# 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 172.16.2.2 [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 **show ip route repair-paths** command shows repair paths marked with the tag [RPR]. The fields in the display are self-explanatory:

```
Device# 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

```

```
Device# 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**

<b>Command</b>	<b>Description</b>
<b>show interfaces tunnel</b>	Displays tunnel interface information.
<b>show ip route summary</b>	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 **show ip route loops** 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 **show ip route loops** 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 **ip route 0.0.0.0 0.0.0.0 192.168.1.2**.

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 **show ip route loops** command to view information about this loop.

## Examples

The following is sample output from the **show ip route loops** 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
	<b>ip route</b>	Establishes static routes.

# show ip route profile

To display routing table change statistics, use the **show ip route profile** command in EXEC mode.

**show ip route profile**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values

**Command Modes** EXEC

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.

## 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 19: 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
<b>ip route profile</b>	Enables IP routing table statistics collection

# show ip route summary

To display the current state of the routing table, use the **show ip routes summary** command in privileged EXEC mode.

**show ip route summary** command **show 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.

## Examples

The following is sample output from the **show ip routes summary** 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           3           360         360
Total           751        17          32130      92160
```

Following table describes the significant fields shown in the display.

**Table 20: 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 <b>connected</b> , <b>static</b> , or <b>internal</b> 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.

Field	Description
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 **show ip routesupernets-only** command in privileged EXEC mode.

**show ip route supernets-only command** `show 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.

## Examples

The following is sample output from the **show ip routesupernets-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 21: show ip route supernets-only Field Descriptions**

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

To display route tag entries for IPv4 routes, use the **show ip route tag** command in user EXEC or privileged EXEC mode.

```
show ip route tag {tag-value | tag-value-dotted-decimal [{mask}]}
```

Syntax Description	Parameter	Description
	<i>tag-value</i>	Route tag value in plain decimals. The range is from 1 to 4294967295.
	<i>tag-value-dotted-decimal</i>	Route tag value in dotted decimals. The range is from 0.0.0.0 to 255.255.255.255.
	<i>mask</i>	(Optional) Route tag wildcard mask.

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

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

**Usage Guidelines** Route tags are 32-bit values attached to routes. They are used to filter routes. You can display route tag values as either plain decimals or dotted decimals.

## Examples

The following sample output from the **show ip route tag** command displays detailed information about route tag entries. The route tag entries in this output are displayed in dotted-decimal format.

```
Device# show ip route tag 1.1.1.1

Routing entry for 192.168.10.0/24
  Known via "eigrp 2", distance 170, metric 1536000
  Tag 1.1.1.1, type external
  Redistributing via eigrp 2
  Last update from 10.0.0.1 on Ethernet0/1, 00:00:20 ago
  Routing Descriptor Blocks:
  * 10.0.0.1, from 10.0.0.1, 00:00:20 ago, via Ethernet0/1
    Route metric is 1536000, traffic share count is 1
    Total delay is 2000 microseconds, minimum bandwidth is 10000 Kbit
    Reliability 100/255, minimum MTU 1500 bytes
    Loading 100/255, Hops 1
    Route tag 1.1.1.1
```

The following sample output from the **show ip route tag** command displays detailed information about route tag entries with the wild card mask. The route tag entries in this output are displayed in dotted-decimal format.

## show ip route tag

```

Device# show ip route tag 10.10.10.0 0.0.0.7

Routing entry for 10.1.10.4/30
  Known via "eigrp 7", distance 170, metric 2560512256
  Tag 10.10.10.3, type external
  Redistributing via eigrp 7, ospf 10
  Last update from 172.16.2.9 on Serial2/1, 00:02:28 ago
  Routing Descriptor Blocks:
  * 172.16.2.9, from 172.16.2.9, 00:02:28 ago, via Serial2/1
    Route metric is 2560512256, traffic share count is 1
    Total delay is 20010 microseconds, minimum bandwidth is 1 Kbit
    Reliability 1/255, minimum MTU 1 bytes
    Loading 1/255, Hops 1
    Route tag 10.10.10.3
Routing entry for 192.168.1.0/24
  Known via "eigrp 7", distance 170, metric 2560512256
  Tag 10.10.10.2, type external
  Redistributing via eigrp 7, ospf 10
  Advertised by ospf 10 metric 100 route-map to_ospf
  Last update from 172.16.2.9 on Serial2/1, 00:01:59 ago
  Routing Descriptor Blocks:
  * 172.16.2.9, from 172.16.2.9, 00:01:59 ago, via Serial2/1
    Route metric is 2560512256, traffic share count is 1
    Total delay is 20010 microseconds, minimum bandwidth is 1 Kbit
    Reliability 1/255, minimum MTU 1 bytes
    Loading 1/255, Hops 1
    Route tag 10.10.10.2
Routing entry for 192.168.2.0/24
  Known via "eigrp 7", distance 170, metric 2560512256
  Tag 10.10.10.2, type external
  Redistributing via eigrp 7, ospf 10
  Advertised by ospf 10 metric 100 route-map to_ospf
  Last update from 172.16.2.9 on Serial2/1, 00:01:59 ago
  Routing Descriptor Blocks:
  * 172.16.2.9, from 172.16.2.9, 00:01:59 ago, via Serial2/1
    Route metric is 2560512256, traffic share count is 1
    Total delay is 20010 microseconds, minimum bandwidth is 1 Kbit
    Reliability 1/255, minimum MTU 1 bytes
    Loading 1/255, Hops 1
    Route tag 10.10.10.2

```

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

**Table 22: show ip route tag Field Descriptions**

Field	Description
Known via	Indicates how the route was derived.
Redistributing via	Indicates the redistribution protocol.
Last update from	Indicates the interface on which the last update arrived.
Routing Descriptor Blocks	Displays the next-hop IP address followed by the information source.
Route metric	Displays the best metric for this routing descriptor block.
Total Delay	Displays the total delay of the route.
Reliability	Indicates the reliability of the link.

Field	Description
Loading	Displays the total load on the link.
Route tag	Displays the tag of the prefix or network.

**Related Commands**

Command	Description
<b>show ipv6 route tags</b>	Displays route tag entries for IPv6 routes.

# show ip route track-table

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

## show ip route track-table

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC (#)

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.

## 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 23: 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
<b>ip route</b>	Establishes static routes in a required network.



# show ip static route

To display the static process local Routing Information Base (RIB) information, use the **show ip static route** 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	Field	Description
	<b>bfd</b>	(Optional) Displays IPv4 static Bidirectional Forwarding Detection (BFD) neighbor information.
	<b>vrf</b> <i>vrf-name</i>	(Optional) Name of the VRF by which static routing information should be displayed.
	<b>topology</b> <i>topology-name</i>	(Optional) Static route information for the specified topology.
	<i>ip-address</i>	(Optional) Address by which static routing information should be displayed.
	<i>mask</i>	(Optional) Subnet mask.
	<b>multicast</b>	(Optional) Displays IPv4 multicast information.
	<b>summary</b>	(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.

## Examples

The following is sample output from the **show ip static route** 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 24: 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 [interface-type interface-number [destination-ip-address]] [group
group-name] [vrf destination-vrf-name] [destination-ip-address [vrf source-vrf-name]
source-ip-address]
```

## Syntax Description

<i>interface-type interface-number</i>	(Optional) Interface type and interface number for which BFD is configured.
<i>destination-ip-address</i>	(Optional) Multihop BFD destination IP address or the gateway IP address.
<b>group</b> <i>group-name</i>	(Optional) Specifies a BFD group and group name.
<b>vrf</b>	(Optional) Specifies the Virtual Routing and Forwarding (VRF) instance.
<i>destination-vrf-name</i>	(Optional) Destination VRF name.
<i>source-vrf-name</i>	(Optional) Source VRF name.
<i>source-ip-address</i>	(Optional) Multihop BFD source IP address.

## Command Modes

User EXEC (>)

Privileged EXEC (#)

## Command History

Release	Modification
15.1(2)S	This command was introduced.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
15.2(3)S	This command was modified. The <b>vrf</b> keyword, and <i>interface-type</i> , <i>interface-number</i> , <i>destination-ip-address</i> , <i>source-ip-address</i> , <i>destination-vrf-name</i> , and <i>source-vrf-name</i> arguments were added.

## 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.

## Examples

Example:

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

```
Device# 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 following table describes the significant fields shown in the display.

**Table 25: show ip static route bfd group Field Descriptions**

Field	Description
GigabitEthernet1/1	Interface for 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 for which the BFD session is initiated.
10.2.2.2	Next-hop IP address.
Passive	Passive member of the group.

#### Related Commands

Command	Description
<b>ip route static bfd</b>	Specifies static route BFD neighbors.
<b>show ip static route</b>	Displays static route database information.

## show ip route vrf

To display the IP routing table associated with a specific VPN routing and forwarding (VRF) instance, use the **show ip route vrf** command in user EXEC or privileged EXEC mode.

```
show ip route vrf {vrf-name | *} [{connected | protocol [{as-number}] | list [{list-number}] | profile |
static | summary | [{ip-prefix|ip-address}] [{mask | longer-prefixes}] | repair-paths | dhcp | supernets-only
| tag {tag-value | tag-value-dotted-decimal [{mask}]}}]
```

### Syntax Description

<i>vrf-name</i> or *	Name of the VRF. Use the asterisk (*) wildcard to include all VRF's.
<b>connected</b>	(Optional) Displays all connected routes in a VRF.
<i>protocol</i>	(Optional) Routing protocol. To specify a routing protocol, use one of the following keywords: <b>bgp</b> , <b>egp</b> , <b>eigrp</b> , <b>hello</b> , <b>igrp</b> , <b>isis</b> , <b>ospf</b> , or <b>rip</b> .
<i>as-number</i>	(Optional) Autonomous system number.
<b>list number</b>	(Optional) Specifies the IP access list to be displayed.
<b>profile</b>	(Optional) Displays the IP routing table profile.
<b>static</b>	(Optional) Displays static routes.
<b>summary</b>	(Optional) Displays a summary of routes.
<i>ip-prefix</i>	(Optional) Network for which routing information is displayed.
<i>ip-address</i>	(Optional) Address for which routing information is displayed.
<i>mask</i>	(Optional) Network mask.
<b>longer-prefixes</b>	(Optional) Displays longer prefix entries.
<b>repair-paths</b>	(Optional) Displays repair paths.
<b>dhcp</b>	(Optional) Displays routes added by the DHCP server.
<b>supernets-only</b>	(Optional) Displays only supernet entries.
<b>tag</b>	(Optional) Displays information about route tags in the VRF table.
<i>tag-value</i>	(Optional) Route tag values as a plain decimals.
<i>tag-value-dotted-decimal</i>	(Optional) Route tag values as a dotted decimals.
<i>mask</i>	(Optional) Route tag wildcard mask.

### Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History	Release	Modification
	12.0(5)T	This command was introduced.
	12.2(2)T	This command was modified. The <i>ip-prefix</i> argument was added. The command output was enhanced to display information on multipaths to the specified network.
	12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
	12.0(22)S	This command was modified. Support for Enhanced Interior Gateway Routing Protocol (EIGRP) VRFs was added.
	12.2(15)T	This command was modified. Support for EIGRP VRFs was added.
	12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH. The output was enhanced to display remote label information and corresponding Multiprotocol Label Switching (MPLS) flags for prefixes that have remote labels stored in the Routing Information Base (RIB).
	12.2(33)SRE	This command was modified. The <b>repair-paths</b> , <b>dhcp</b> , and <b>supernets-only</b> 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 integrated into Cisco IOS XE Release 2.5.
	15.2(2)S	This command was modified. The <b>tag</b> keyword and <i>tag-value</i> , <i>tag-value-dotted-decimal</i> , and <i>mask</i> arguments were added to enable the display of route tags as plain or dotted decimals in the command output.
	Cisco IOS XE Release 3.6S	This command was modified. The <b>tag</b> keyword and <i>tag-value</i> , <i>tag-value-dotted-decimal</i> , and <i>mask</i> arguments were added to enable the display of route tags as plain or dotted decimals in the command output.
	15.2(4)S	This command was implemented on the Cisco 7200 series router.
	15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
	IOS XE Gibraltar 16.12.1	Extended use of asterisk (*) wildcard for <i>vrf-name</i> to work with the <b>summary</b> keyword.

## Examples

The following sample output displays the IP routing table associated with the VRF named vrf1:

```
Device# show ip route vrf vrf1
```

```
Codes: C - connected, S - static, I - IGRP, 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, E - EGP
I - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
U - per-user static route, o - ODR
T - traffic engineered route

```

Gateway of last resort is not set

```

B 10.0.0.0/8 [200/0] via 10.13.13.13, 00:24:19
C 10.0.0.0/8 is directly connected, Ethernet1/3
B 10.0.0.0/8 [20/0] via 10.0.0.1, 02:10:22
B 10.0.0.0/8 [200/0] via 10.13.13.13, 00:24:20

```

This following sample output shows BGP entries in the IP routing table associated with the VRF named vrf1:

```
Device# show ip route vrf vrf1 bgp
```

```

B 10.0.0.0/8 [200/0] via 10.13.13.13, 03:44:14
B 10.0.0.0/8 [20/0] via 10.0.0.1, 03:44:12
B 10.0.0.0/8 [200/0] via 10.13.13.13, 03:43:14

```

The following sample output displays the IP routing table associated with a VRF named PATH:

```
Device# show ip route vrf PATH 10.22.22.0
```

```

Routing entry for 10.22.22.0/24
  Known via "bgp 1", distance 200, metric 0
  Tag 22, type internal
  Last update from 10.22.5.10 00:01:07 ago
  Routing Descriptor Blocks:
  * 10.22.7.8 (Default-IP-Routing-Table), from 10.11.3.4, 00:01:07 ago
    Route metric is 0, traffic share count is 1
    AS Hops 1
  10.22.1.9 (Default-IP-Routing-Table), from 10.11.1.2, 00:01:07 ago
    Route metric is 0, traffic share count is 1
    AS Hops 1
  10.22.6.10 (Default-IP-Routing-Table), from 10.11.6.7, 00:01:07 ago
    Route metric is 0, traffic share count is 1
    AS Hops 1
  10.22.4.10 (Default-IP-Routing-Table), from 10.11.4.5, 00:01:07 ago
    Route metric is 0, traffic share count is 1
    AS Hops 1
  10.22.5.10 (Default-IP-Routing-Table), from 10.11.5.6, 00:01:07 ago
    Route metric is 0, traffic share count is 1
    AS Hops 1

```

The following sample output from the **show ip route vrf vrf-name tag** command displays route tag information for routes associated with vrf1. The route tags in the sample output are displayed in dotted decimal format.

```
Device# show ip route vrf vrf1 tag 5
```

```

Routing Table: vrf1
Routing entry for 10.0.0.1/24
  Known via "static", distance 1, metric 0 (connected)
  Tag 0.0.0.5
  Routing Descriptor Blocks:
  * directly connected, via Null0
    Route metric is 0, traffic share count is 1
    Route tag 0.0.0.5

```

The following sample outputs from the **show ip route vrf** command include recursive-via-host and recursive-via-connected flags:

```
Device# show ip route vrf v2 10.2.2.2

Routing Table: v2
Routing entry for 10.2.2.2/32
  Known via "bgp 10", distance 20, metric 0
  Tag 100, type external
  Last update from 192.168.1.1 00:15:54 ago
  Routing Descriptor Blocks:
  * 192.168.1.1, from 192.168.1.1, 00:15:54 ago, recursive-via-conn
    Route metric is 0, traffic share count is 1
    AS Hops 1
    Route tag 100
    MPLS label: none

Device# show ip route vrf v2 10.2.2.2

Routing Table: v2
Routing entry for 10.2.2.2/32
  Known via "bgp 10", distance 200, metric 0
  Tag 100, type internal
  Last update from 10.3.3.3 00:18:11 ago
  Routing Descriptor Blocks:
  * 10.3.3.3 (default), from 10.5.5.5, 00:18:11 ago, recursive-via-host
    Route metric is 0, traffic share count is 1
    AS Hops 1
    Route tag 100
    MPLS label: 16
    MPLS Flags: MPLS Required
```

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

**Table 26: show ip route vrf Field Descriptions**

Field	Description
Routing entry for 10.22.22.0/24	Network number.
Known via ...	Indicates how the route was derived.
distance	Administrative distance of the information source.
metric	Metric used to reach the destination network.
Tag	Integer used to tag the route.
type	Indicates whether the route is an L1 type or L2 type of route.
Last update from 10.22.5.10	Indicates the IP address of the device that is the next hop to the remote network and identifies the interface on which the last update arrived.
00:01:07 ago	Specifies the last time the route was updated (in hours:minutes:seconds).
Routing Descriptor Blocks	Displays the next-hop IP address followed by the information source.

Field	Description
10.22.6.10, from 10.11.6.7, 00:01:07 ago	Indicates the next-hop address, the address of the gateway that sent the update, and the time that has elapsed since this update was received (in hours:minutes:seconds).
Route metric	This value is the best metric for this routing descriptor block.
Traffic share count	Indicates the number of packets transmitted over various routes.
AS Hops	Number of hops to the destination or to the device where the route first enters internal BGP (iBGP).

The following is sample output from the **show ip route vrf** command on devices using the Cisco IOS Software Modularity for Layer 3 VPNs feature. The output includes remote label information and corresponding MPLS flags for prefixes that have remote labels stored in the RIB if BGP is the label distribution protocol.

```
Device# show ip route vrf v2 10.2.2.2

Routing entry for 10.2.2.2/32
  Known via "bgp 1", distance 200, metric 0, type internal
  Redistributing via ospf 2
  Advertised by ospf 2 subnets
  Last update from 10.0.0.4 00:22:59 ago
  Routing Descriptor Blocks:
  * 10.0.0.4 (Default-IP-Routing-Table), from 10.0.0.31, 00:22:59 ago
    Route metric is 0, traffic share count is 1
    AS Hops 0
    MPLS label: 1300
    MPLS Flags: MPLS Required
```

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

**Table 27: show ip route vrf Field Descriptions**

Field	Description
MPLS label	<p>Displays the BGP prefix from the BGP peer. The output shows one of the following values:</p> <ul style="list-style-type: none"> <li>• A label value (16–1048575).</li> <li>• A reserved label value, such as explicit-null or implicit-null.</li> <li>• The word “none” if no label is received from the peer.</li> </ul> <p>The MPLS label field is not displayed if any of the following conditions is true:</p> <ul style="list-style-type: none"> <li>• BGP is not the Label Distribution Protocol (LDP). However, Open Shortest Path First (OSPF) prefixes learned via sham links display an MPLS label.</li> <li>• MPLS is not supported.</li> <li>• The prefix is imported from another VRF, where the prefix was an Interior Gateway Protocol (IGP) prefix and LDP provided the remote label for it.</li> </ul>



Field	Description
MPLS Flags	<p>Name of the MPLS flag. One of the following MPLS flags is displayed:</p> <ul style="list-style-type: none"> <li>• <b>MPLS Required</b>—Indicates that packets are forwarded to this prefix because of the presence of the MPLS label stack. If MPLS is disabled on the outgoing interface, the packets are dropped.</li> <li>• <b>No Global</b>—Indicates that MPLS packets for this prefix are forwarded from the VRF interface and not from the interface in the global table. VRF interfaces prevent loops in scenarios that use iBGP multipaths.</li> <li>• <b>NSF</b>—Indicates that the prefix is from a nonstop forwarding (NSF)-aware neighbor. If the routing information temporarily disappears due to a disruption in the control plane, packets for this prefix are preserved.</li> </ul>

The following sample output from the **show ip route vrf** command shows repair paths in the routing table. The fields in the display are self-explanatory.

```
Device> show ip route vrf test1 repair-paths 192.168.3.0

Routing Table: test1
Routing entry for 192.168.3.0/24
  Known via "bgp 10", distance 20, metric 0
  Tag 100, type external
  Last update from 192.168.1.1 00:49:39 ago
  Routing Descriptor Blocks:
  * 192.168.1.1, from 192.168.1.1, 00:49:39 ago, recursive-via-conn
    Route metric is 0, traffic share count is 1
    AS Hops 1
    Route tag 100
    MPLS label: none
  [RPR]10.4.4.4 (default), from 10.5.5.5, 00:49:39 ago, recursive-via-host
    Route metric is 0, traffic share count is 1
    AS Hops 1
    Route tag 100
    MPLS label: 29
MPLS Flags: MPLS Required, No Global
```

### Using wildcard for VRF name

This example uses the asterisk (\*) wildcard for *vrf-name*, with the **summary** keyword. All VRF's are included, in this case default, blue, and red.

```
Device#show ip route vrf * summary
IP routing table name is default (0x0)
IP routing table maximum-paths is 32
Route Source    Networks    Subnets    Replicates    Overhead    Memory (bytes)
application     0           0           0             0           0
connected      0           2           0            192         624
static         1           1           0            192         624
internal       1           1           0             672
Total          2           3           0            384        1920

IP routing table name is blue (0x2)
IP routing table maximum-paths is 32
Route Source    Networks    Subnets    Replicates    Overhead    Memory (bytes)
```

**show ip route vrf**

```

application      0          0          0          0          0
connected        0          0          0          0          0
static           0          0          0          0          0
internal         0          0          0          0          40
Total            0          0          0          0          40

```

IP routing table name is red (0x5)

IP routing table maximum-paths is 32

```

Route Source   Networks   Subnets   Replicates   Overhead   Memory (bytes)
application    0          0          0             0           0
connected      0          0          0             0           0
static         0          0          0             0           0
internal       0          0          0             0           40
Total          0          0          0             0           40

```

**Related Commands**

Command	Description
<b>show ip cache</b>	Displays the Cisco Express Forwarding table associated with a VRF.
<b>show ip vrf</b>	Displays the set of defined VRFs and associated interfaces.

# show ipv6 policy

To display the IPv6 policy-based routing (PBR) configuration, use the **show ipv6 policy** command in user EXEC or privileged EXEC mode.

**show ipv6 policy**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

User EXEC

Privileged EXEC

## Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(33)SX14	This command was integrated into Cisco IOS Release 12.2(33)SX14.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

## Usage Guidelines

IPv6 policy matches will be counted on route maps, as is done in IPv4. Therefore, IPv6 policy matches can also be displayed on the **show route-map** command.

## Examples

The following example displays the PBR configuration:

```
Device# show ipv6 policy

Interface          Routemap
Ethernet0/0        src-1
```

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

Field	Description
Interface	Interface type and number that is configured to run Protocol-Independent Multicast (PIM).
Routemap	The name of the route map on which IPv6 policy matches were counted.

## Related Commands

Command	Description
<b>show route-map</b>	Displays all route maps configured or only the one specified.

## show ipv6 route

To display contents of the IPv6 routing table, use the **show ipv6 route** command in user EXEC or privileged EXEC mode.

```
show ipv6 route [{ipv6-address | ipv6-prefix/prefix-length [longer-prefixes]}] [{protocol}] | [repair]
| [{updated [boot-up] [day month] [time]}] | interface type number | nd | nsf | table table-id |
watch}]
```

### Syntax Description

<i>ipv6-address</i>	(Optional) Displays routing information for a specific IPv6 address.
<i>ipv6-prefix</i>	(Optional) Displays routing information for a specific IPv6 network.
<i>/prefix-length</i>	(Optional) The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
<b>longer-prefixes</b>	(Optional) Displays output for longer prefix entries.
<i>protocol</i>	(Optional) The name of a routing protocol or the keyword <b>connected</b> , <b>local</b> , <b>mobile</b> , or <b>static</b> . If you specify a routing protocol, use one of the following keywords: <b>bgp</b> , <b>isis</b> , <b>eigrp</b> , <b>ospf</b> , or <b>rip</b> .
<b>repair</b>	(Optional) Displays routes with repair paths.
<b>updated</b>	(Optional) Displays routes with time stamps.
<b>boot-up</b>	(Optional) Displays routing information since bootup.
<i>day month</i>	(Optional) Displays routes since the specified day and month.
<i>time</i>	(Optional) Displays routes since the specified time, in <i>hh:mm</i> format.
<b>interface</b>	(Optional) Displays information about the interface.
<i>type</i>	(Optional) Interface type.
<i>number</i>	(Optional) Interface number.
<b>nd</b>	(Optional) Displays only routes from the IPv6 Routing Information Base (RIB) that are owned by Neighbor Discovery (ND).
<b>nsf</b>	(Optional) Displays routes in the nonstop forwarding (NSF) state.
<b>repair</b>	(Optional)
<b>table</b> <i>table-id</i>	(Optional) Displays IPv6 RIB table information for the specified table ID. The table ID must be in hexadecimal format. The range is from 0 to 0-0xFFFFFFFF.
<b>watch</b>	(Optional) Displays information about route watchers.

**Command Default** If none of the optional syntax elements is chosen, all IPv6 routing information for all active routing tables is displayed.

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

Command History	Release	Modification
	12.2(2)T	This command was introduced.
	12.2(8)T	This command was modified. The <b>isis</b> keyword was added, and the I1 - ISIS L1, I2 - ISIS L2, and IA - ISIS interarea fields were included in the command output.
	12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
	12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S. The timer information was removed, and an indicator was added to display IPv6 Multiprotocol Label Switching (MPLS) interfaces.
	12.2(13)T	This command was modified. The timer information was removed, and an indicator was added to display IPv6 MPLS virtual interfaces.
	12.2(14)S	This command was modified. The <b>longer-prefixes</b> keyword was added.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
	12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
	Cisco IOS XE Release 2.1	This command was implemented on Cisco ASR 1000 Series Aggregation Services Routers.
	12.4(24)T	This command was modified in a release earlier than Cisco IOS Release 12.4(24)T. The <b>table</b> , <b>nsf</b> , <b>watch</b> , and <b>updated</b> keywords and the <i>day</i> , <i>month</i> , <i>table-id</i> , and <i>time</i> arguments were added.
	15.2(2)S	This command was modified. The command output was enhanced to include route tag values in dotted-decimal format.
	Cisco IOS XE Release 3.6S	This command was modified. The command output was enhanced to include route tag values in dotted-decimal format.
	15.1(1)SY	The <b>nd</b> keyword was added.
	Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.
	15.2(2)SA2	This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches.

**Usage Guidelines**

The **show ipv6 route** command provides output similar to the **show ip route** command, except that the information is IPv6-specific.

When the *ipv6-address* or *ipv6-prefix/prefix-length* argument is specified, the longest match lookup is performed from the routing table, and only route information for that address or network is displayed. When a routing protocol is specified, only routes for that protocol are displayed. When the **connected**, **local**, **mobile**, or **static** keyword is specified, only the specified type of route is displayed. When the **interface** keyword and *type* and *number* arguments are specified, only routes for the specified interface are displayed.

**Examples**

The following is sample output from the **show ipv6 route** command when no keywords or arguments are specified:

```
Device# show ipv6 route

IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       I1 - ISIS L1, I2 - ISIS L2, IA - IIS interarea
B   2001:DB8:4::2/48 [20/0]
    via FE80::A8BB:CCFF:FE02:8B00, Serial6/0
L   2001:DB8:4::3/48 [0/0]
    via ::, Ethernet1/0
C   2001:DB8:4::4/48 [0/0]
    via ::, Ethernet1/0
LC  2001:DB8:4::5/48 [0/0]
    via ::, Loopback0
L   2001:DB8:4::6/48 [0/0]
    via ::, Serial6/0
C   2001:DB8:4::7/48 [0/0]
    via ::, Serial6/0
S   2001:DB8:4::8/48 [1/0]
    via 2001:DB8:1::1, Null
L   FE80::/10 [0/0]
    via ::, Null0
L   FF00::/8 [0/0]
    via ::, Null0
```

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

**Table 28: show ipv6 route Field Descriptions**

Field	Description
Codes:	<p>Indicates the protocol that derived the route. Values are as follows:</p> <ul style="list-style-type: none"> <li>• B—BGP derived</li> <li>• C—Connected</li> <li>• I1—ISIS L1—Integrated IS-IS Level 1 derived</li> <li>• I2—ISIS L2—Integrated IS-IS Level 2 derived</li> <li>• IA—ISIS interarea—Integrated IS-IS interarea derived</li> <li>• L—Local</li> <li>• R—RIP derived</li> <li>• S—Static</li> </ul>

Field	Description
2001:DB8:4::2/48	Indicates the IPv6 prefix of the remote network.
[20/0]	The first number in brackets is the administrative distance of the information source; the second number is the metric for the route.
via FE80::A8BB:CCFF:FE02:8B00	Specifies the address of the next device to the remote network.

When the *ipv6-address* or *ipv6-prefix/prefix-length* argument is specified, only route information for that address or network is displayed. The following is sample output from the **show ipv6 route** command when IPv6 prefix 2001:DB8::/35 is specified. The fields in the display are self-explanatory.

```
Device# show ipv6 route 2001:DB8::/35

IPv6 Routing Table - 261 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
B 2001:DB8::/35 [20/3]
  via FE80::60:5C59:9E00:16, Tunnel1
```

When you specify a protocol, only routes for that particular routing protocol are shown. The following is sample output from the **show ipv6 route bgp** command. The fields in the display are self-explanatory.

```
Device# show ipv6 route bgp

IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
      I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
B   2001:DB8:4::4/64 [20/0]
    via FE80::A8BB:CCFF:FE02:8B00, Serial6/0
```

The following is sample output from the **show ipv6 route local** command. The fields in the display are self-explanatory.

```
Device# show ipv6 route local

IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
      I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
L   2001:DB8:4::2/128 [0/0]
    via ::, Ethernet1/0
LC  2001:DB8:4::1/128 [0/0]
    via ::, Loopback0
L   2001:DB8:4::3/128 [0/0]
    via ::, Serial6/0
L   FE80::/10 [0/0]
    via ::, Null0
L   FF00::/8 [0/0]
    via ::, Null0
```

The following is sample output from the **show ipv6 route** command when the 6PE multipath feature is enabled. The fields in the display are self-explanatory.

```
Device# show ipv6 route
```

## show ipv6 route

```

IPv6 Routing Table - default - 19 entries
Codes:C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       .
       .
       .
B      2001:DB8::/64 [200/0]
       via ::FFFF:172.16.0.1
       via ::FFFF:172.30.30.1

```

## Related Commands

Command	Description
<b>ipv6 route</b>	Establishes a static IPv6 route.
<b>show ipv6 interface</b>	Displays IPv6 interface information.
<b>show ipv6 route summary</b>	Displays the current contents of the IPv6 routing table in summary format.
<b>show ipv6 tunnel</b>	Displays IPv6 tunnel information.



# show ipv6 route shortcut

To display the IPv6 routes that contain shortcuts, use the **show ipv6 route shortcut** command in privileged EXEC mode.

**show ipv6 route shortcut**

## Syntax Description

This command has no arguments or keywords.

## Command Default

IPv6 information about shortcuts for all active routing tables is displayed.

## Command Modes

Privileged EXEC (#)

## Command History

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

## Usage Guidelines

The **show ipv6 route shortcut** command displays only the routes that have overriding shortcut paths.

## Examples

The following is sample output from the **show ipv6 route shortcut** command:

```
Router# show ipv6 route shortcut
IPv6 Routing Table - default - 7 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO
       ND - Neighbor Discovery, l - LISP
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
S 7000:1::/64 [1/0]
  via 4000:1:1::1, Ethernet1/1 [Shortcut]
  via 5000:1:1::1, Ethernet1/1 [Shortcut]
  via Ethernet1/1, directly connected
S 8000:1:1::/64 [1/0]
  via 6000:1:1::1, Ethernet0/1 [Shortcut]
  via Ethernet0/0, directly connected
```

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

Table 29: show ipv6 route shortcut Field Descriptions

Field	Description
Codes:	Indicates the protocol that derived the route. Values are as follows: <ul style="list-style-type: none"> <li>• C--Connected</li> <li>• L--Local</li> <li>• S--Static</li> <li>• R--RIP derived</li> <li>• B--BGP derived</li> <li>• I1--ISIS L1--Integrated IS-IS Level 1 derived</li> <li>• I2--ISIS L2--Integrated IS-IS Level 2 derived</li> <li>• IA--ISIS interarea--Integrated IS-IS interarea derived</li> </ul>
S 7000:1::/64 [1/0]	Indicates paths that may be shortcut paths.
via 4000:1:1::1, Ethernet1/1	Indicates a path that may be a shortcut path.
via 5000:1:1::1, Ethernet1/1 [Shortcut]	Indicates a path that may be a shortcut path.
via Ethernet1/1, directly connected	Shows routes connected to the router directly.

**Related Commands**

Command	Description
<b>ipv6 route</b>	Establishes a static IPv6 route.
<b>show ipv6 interface</b>	Displays IPv6 interface information.
<b>show ipv6 route summary</b>	Displays the current contents of the IPv6 routing table in summary format.
<b>show ipv6 tunnel</b>	Displays IPv6 tunnel information.

# show ipv6 route summary

To display the current contents of the IPv6 routing table in summary format, use the **show ipv6 route summary** command in user EXEC or privileged EXEC mode.

**show ipv6 route summary**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

User EXEC  
Privileged EXEC

## Command History

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

## Examples

The following is sample output from the **show ipv6 route summary** command:

```
Router# show ipv6 route summary
IPv6 Routing Table Summary - 257 entries
 37 local, 35 connected, 25 static, 0 RIP, 160 BGP
Number of prefixes:
  /16: 1, /24: 46, /28: 10, /32: 5, /35: 25, /40: 1, /48: 63, /64: 19
  /96: 15, /112: 1, /126: 31, /127: 4, /128: 36
```

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

**Table 30: show ipv6 route summary Field Descriptions**

Field	Description
entries	Number of entries in the IPv6 routing table.

## show ipv6 route summary

Field	Description
Route source	Number of routes that are present in the routing table for each route source, which can be local routes, connected routes, static routes, a routing protocol, prefix and address or name, and longer prefixes and address or name.  Routing protocols can include RIP, IS-IS, OSPF, and BGP.  Other route sources can be connected, local, static, or a specific interface.
Number of prefixes:	Number of routing table entries for given prefix length.

## Related Commands

Command	Description
<b>show ipv6 route</b>	Displays the current contents of the IPv6 routing table.

# show ipv6 route tag

To display route tag entries for IPv6 routes, use the **show ipv6 route tag** command in user EXEC or privileged EXEC mode.

```
show ipv6 route tag {tag-value | tag-value-dotted-decimal [{mask}]}
```

Syntax Description	Parameter	Description
	<i>tag-value</i>	Route tag value in plain decimals. The range is from 1 to 4294967295.
	<i>tag-value-dotted-decimal</i>	Route tag value in dotted decimals. The range is from 0.0.0.0 to 255.255.255.255.
	<i>mask</i>	(Optional) Route tag wildcard mask.

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

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

**Usage Guidelines** Route tags are 32-bit values attached to routes. They are used to filter routes. You can display route tag entries as either plain decimals or dotted decimals.

## Examples

The following sample output from the **show ipv6 route tag** command displays detailed information about route tag entries in the routing table. Route tag values in this output are displayed in dotted-decimal format.

```
Device# show ipv6 route tag 0.0.10.10

IPv6 Routing Table - default - 4 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE -
Destination
       NDr - Redirect, l - LISP
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
R 2001:DB8::/96 [120/2]
  Tag 0.0.10.10
  via FE80::A8BB:CCFF:FE00:A00, Ethernet0/0
```

The following sample output from the **show ipv6 route tag** command displays detailed information about route tag entries with the wild card mask. Route tag values in this output are displayed in dotted-decimal format.

## show ipv6 route tag

```

Device# show ipv6 route tag 0.0.0.10 0.0.0.7

IPv6 Routing Table - default - 4 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, l - LISP
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
R    2001:DB8::/32 [0/0]
    Tag 0.0.0.10
    via FE80::A8BB:CCFF:FE00:A00, Ethernet0/0

```

The table below describes the significant fields in the displays.

**Table 31: show ipv6 route tag Field Descriptions**

Field	Description
Codes	Indicates the protocol that derived the route. It can be one of the following values: <ul style="list-style-type: none"> <li>• B—BGP derived</li> <li>• C—Connected</li> <li>• D—Enhanced Interior Gateway Routing Protocol (EIGRP)</li> <li>• EX—EIGRP external</li> <li>• H—NHRP</li> <li>• i—IS-IS derived</li> <li>• L—Local</li> <li>• O—Open Shortest Path First (OSPF) derived</li> <li>• P—Periodic downloaded static route</li> <li>• R—Routing Information Protocol (RIP) derived</li> <li>• S—Static</li> <li>• U—Per-user static route</li> </ul>
2001:DB8::/96 [120/2]	Indicates the address of the remote network.
Tag	Identifies the tag associated with the remote network.
via FE80::A8BB:CCFF:FE00:A00	Specifies the IPv6 address of the next router to the remote network.
Ethernet0/0	Specifies the interface through which the specified network can be reached.

### Related Commands

Command	Description
<b>show ip route tag</b>	Displays route tag entries for IPv4 routes.

# show ipv6 route vrf

To display IPv6 routing table information associated with a VPN routing and forwarding (VRF) instance, use the **show ipv6 route vrf** command in user EXEC or privileged EXEC mode.

```
show ipv6 route vrf {vrf-name|vrf-number}[tag {tag-value | tag-value-dotted-decimal [{mask}]]]
```

Syntax Description		
<i>vrf-name</i>		Name assigned to the VRF.
<i>vrf-number</i>		Hexadecimal number assigned to the VRF.
<b>tag</b>		(Optional) Displays information about route tags in the VRF table.
<i>tag-value</i>		(Optional) Displays route tag value in plain decimals.
<i>tag-value-dotted-decimal</i>		(Optional) Displays route tag values in dotted decimals.
<i>mask</i>		(Optional) Route tag wildcard mask.

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

Command History	Release	Modification
	12.2(33)SRB	This command was introduced.
	12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
	12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
	15.2(2)S	This command was integrated into Cisco IOS Release 15.2(2)S. The <b>tag</b> keyword and the <i>tag-value</i> , <i>tag-value-dotted-decimal</i> , and <i>mask</i> arguments were added to enable the display of route tags as plain decimals or dotted decimals in the command output.
	Cisco IOS XE Release 3.6S	This command was integrated into Cisco IOS XE Release 3.6S. The <b>tag</b> keyword and the <i>tag-value</i> , <i>tag-value-dotted-decimal</i> , and <i>mask</i> arguments were added to enable the display of route tags as plain decimals or dotted decimals in the command output.
	15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.
	15.2(2)SNI	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

## Examples

The following sample output from the **show ipv6 route vrf** command displays information about the IPv6 routing table associated with VRF1:

```
Device# show ipv6 route vrf VRF1
```

## show ipv6 route vrf

```

IPv6 Routing Table VRF1 - 6 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
        U - Per-user Static route
        I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
        O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
C 2001:DB8:4::2/48 [0/0]
   via ::, FastEthernet0/0
L 2001:DB8:4::3/48 [0/0]
   via ::, FastEthernet0/0
B 2001:DB8:4::4/48 [200/0]
   via ::FFFF:192.168.1.4,
B 2001:DB8:4::5/48 [20/1]
   via 2001:8::1,
C 2001:DB8:4::6/48 [0/0]
   via ::, Loopback1
L 2001:DB8:4::7/48 [0/0]
   via ::, Loopback1

```

The following sample output from the **show ip route vrf vrf-name tag** command displays information about tagged IPv6 routes in vrf1:

```

Device# show ipv6 route vrf vrf1 tag 0.0.0.6

IPv6 Routing Table - vrf1 - 2 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
        B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
        I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
        EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
        NDr - Redirect, l - LISP
        O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
        ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
Routing entry for 2001::/32
  Known via "static", distance 1, metric 0
  Tag 0.0.0.6
  Route count is 1/1, share count 0
  Routing paths:
    directly connected via Null0
    Last updated 00:00:23 ago

```

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



Table 32: show ipv6 route vrf Field Descriptions

Field	Description
Codes	<p>Indicates the protocol that derived the route. It can be one of the following values:</p> <ul style="list-style-type: none"> <li>• B—BGP derived</li> <li>• C—Connected</li> <li>• D—Enhanced Interior Gateway Routing Protocol (EIGRP)</li> <li>• EX—EIGRP external</li> <li>• H—NHRP</li> <li>• I—IS-IS derived</li> <li>• L—Local</li> <li>• O—Open Shortest Path First (OSPF) derived</li> <li>• P—Periodic downloaded static route</li> <li>• R—Routing Information Protocol (RIP) derived</li> <li>• S—Static</li> <li>• U—Per-user static route</li> </ul>
via ::, FastEthernet0/0	Indicates how the route was derived.
Tag	Identifies the tag associated with the remote network.

## 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** | **remote-lfa tunnels**}

### Syntax Description

<b>interfaces</b>	Displays information about platform support capability for all interfaces running IS-IS.
<i>type</i>	(Optional) Interface type. For more information, use the question mark (?) online help function.
<i>number</i>	(Optional) Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
<b>summary</b>	Displays FRR configuration information summary.
<b>remote-lfa tunnels</b>	Displays information about remote loop-free alternate (LFA) tunnels.

### 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.
15.2(2)S	This command was modified. The <b>remote-lfa tunnels</b> keyword was added.
15.2(2)SNI	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

### Usage Guidelines

The **show isis fast-reroute** command displays whether an interface is supported by a platform.

### 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 33: show isis fast-reroute interfaces Field Descriptions**

Field	Description
Protectable	Specifies whether an interface is supported by the platform to be protected by FRR.
Usable for repair	Specifies whether an interface is supported by the platform to be used as a repair path.



**Note** Whether an interface is actually FRR protected or is acting as an FRR repair interface depends on the topology and the configuration. The information in the **show isis fast-reroute interfaces** command shows only the capability of the interface as supported by the platform.

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 34: 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.

The following is sample output from the **show isis fast-reroute remote-lfa tunnels** command:

```
Router# show isis fast-reroute remote-lfa tunnels

Tag Null - Fast-Reroute Remote-LFA Tunnels:

MPLS-Remote-Lfa1: use Et1/0, nexthop 10.0.0.1, end point 24.24.24.24
MPLS-Remote-Lfa2: use Et0/0, nexthop 10.1.1.2, end point 24.24.24.24
```

**Related Commands**

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

# show key chain

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

**show key chain command** `show key chain [name-of-chain]`

<b>Syntax Description</b>	<i>name-of-chain</i> (Optional) Name of the key chain to display, as named in the <b>keychain</b> command.
---------------------------	--

**Command Default** Information about all key chains is displayed.

**Command Modes** EXEC

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	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.

## 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)
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>accept-lifetime</b>	Sets the time period during which the authentication key on a key chain is received as valid.
	<b>key</b>	Identifies an authentication key on a key chain.
	<b>key chain</b>	Enables authentication for routing protocols.
	<b>key-string (authentication)</b>	Specifies the authentication string for a key.
	<b>send-lifetime</b>	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 **show monitor event-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		
<b>all-traces</b>		(Optional) Displays all event trace messages in memory to the console.
<i>component</i>		(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 <b>monitorevent-trace?</b> command.
<b>all</b>		Displays all event trace messages currently in memory for the specified component.
<b>back</b> <i>hour:minute</i>		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).
<b>clock</b> <i>hour:minute</i>		Displays event trace messages starting from a specific clock time in hours and minutes format (hh:mm).
<b>from-boot</b> <i>seconds</i>		Displays event trace messages starting from a specified number of seconds after booting (uptime). To display the uptime, in seconds, enter the <b>showmonitorevent-tracecomponentfrom-boot?</b> command.
<b>latest</b>		Displays only the event trace messages since the last <b>showmonitorevent-trace</b> command was entered.
<b>parameters</b>		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 <b>showmonitorevent-tracecef</b> command replaced the <b>showcefevents</b> and <b>showipcefevents</b> commands.
	12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.  The <b>spa</b> component keyword was added to support online insertion and removal (OIR) event messages for shared port adapters (SPAs).  The <b>bfd</b> keyword was added for the <i>component</i> argument to display trace messages relating to the Bidirectional Forwarding Detection (BFD) feature.

Release	Modification
12.4(4)T	Support for the <b>bfd</b> keyword was added for Cisco IOS Release 12.4(4)T.
12.0(31)S	Support for the <b>bfd</b> 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 <b>cfid</b> keyword was added as an entry for the <i>component</i> 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 **cfid** 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.

### Examples

#### IPC Component Example

The following is sample output from the **showmonitorevent-tracecomponent** 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
```

#### BFD Component for Cisco IOS Release 12.2(18)SXE, 12.0(31)S, and 12.4(4)T

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

```

### SPA Component Example

The following is sample output from the **showmonitorevent-tracecomponentlatest** 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

```

### Cisco Express Forwarding Component 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
```



### Cisco Express Forwarding Component Examples for Cisco 10000 Series Routers Only

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
```

### CFD Component for Cisco IOS Release 12.4(9)T

To troubleshoot errors in an encryption datapath, enter the `show monitor event-trace cef crypto` command. This command displays the events for the Cisco Express Forwarding component for the Cisco Confidential (CFD) component.



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

## show monitor event-trace

```

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
<b>monitor event-trace (EXEC)</b>	Controls event trace functions for a specified Cisco IOS software subsystem component.
<b>monitor event-trace (global)</b>	Configures event tracing for a specified Cisco IOS software subsystem component.
<b>monitor event-trace dump-traces</b>	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 **show platform hardware qfp active feature cef-mpls prefix ip** command in privileged EXEC.

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

Syntax Description	
<i>ipv4 prefix</i>	IPv4 address and mask.
<b>vrf</b>	(Optional) Displays information about VPN Routing and Forwarding (VRF).
<i>id</i>	(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.
<b>exact</b>	(Optional) Find and displays the exact match of the IPV4 prefix.
<b>brief</b>	(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.

## Examples

The following is sample output from the **show platform hardware qfp active feature cef-mpls prefix ip** 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
```

**show platform hardware qfp active feature cef-mpls prefix ip**

```

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

<i>ipv6-prefix</i>	IPv6 address and prefix. The IPv6 prefix is in the range from 0 to 128.
<b>vrf</b> <i>id</i>	(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.
<b>exact</b>	(Optional) Finds and displays the exact match of the IPv6 prefix.
<b>brief</b>	(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.

## 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
```

## show platform hardware qfp active feature cef-mpls prefix ipv6

```
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		
	<i>label</i>	Multiprotocol Label Switching (MPLS) label. The range is from 0 to 1048575.
	<b>vrf</b>	(Optional) Displays information about VPN Routing and Forwarding (VRF).
	<i>id</i>	(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.
	<b>exact</b>	(Optional) Finds and displays the exact match of the prefix.
	<b>brief</b>	(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.

## 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 ===
```

## show platform hardware qfp active feature cef-mpls prefix mpls

```

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 platform software ip fp active cloudsec

To display the configuration information for CloudSec padding-fixup in the Embedded-Service-Processor, use the **show platform software ip fp active cloudsec** command in privileged EXEC mode.

```
show platform software ip fp active cloudsec
```

**Command Modes** Privileged EXEC (#)

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

## Examples

The following is a sample output from the **show platform software ip fp active cloudsec** command:

```
Router# show platform software ip fp active cloudsec
CloudSec Debug: enabled
  CloudSec UDP destination port: enabled
    1st UDP destination port: 9999
    2nd UDP destination port: 5120
    3rd UDP destination port: 8017
```

# show platform software ip rp active cloudsec

To display the configuration information for CloudSec padding-fixup in Route Processor, use the **show platform software ip rp active cloudsec** command in privileged EXEC mode.

```
show platform software ip rp active cloudsec
```

## Command Modes

Privileged EXEC (#)

## Command History

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

## Examples

The following is a sample output from the **show platform software ip rp active cloudsec** command:

```
Router# show platform software ip rp active cloudsec
CloudSec Debug: enabled
  CloudSec UDP destination port: enabled
    1st UDP destination port: 9999
    2nd UDP destination port: 5120
    3rd UDP destination port: 8017
```

# show route-map

To display static and dynamic route maps configured on the router, use the **show route-map** command in user EXEC or privileged EXEC mode.

```
show route-map [{map-name | dynamic [{dynamic-map-name | application [application-name]}] | all}
[detailed]
```

## Syntax Description

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

## Command Modes

User EXEC (>)

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 included in the command output.
12.2(27)SBA	This command was modified. The output was enhanced to display dynamically assigned route maps in VPN routing and forwarding (VRF) tables.
12.2(15)T	This command was modified. An additional counter-collect policy routing statistic was added to the command output.
12.3(2)T	This command was modified. Support for Continue clauses was included in the command output.
12.2(17b)SXA	This command was integrated into Cisco IOS Release 12.2(17b)SXA.
12.3(7)T	This command was modified. The <b>dynamic</b> , <b>application</b> , and <b>all</b> keywords were added.
12.0(28)S	This command was modified. Support for the recursive next-hop clause was added to the command output.

Release	Modification
12.3(14)T	This command was modified. Support for the recursive next-hop clause, map display extension functionality, and the <b>detailed</b> keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2.
15.0(1)M	This command was modified. The <b>detailed</b> keyword was removed.
15.2(2)S	This command was modified. The command output was enhanced to display route tag values in dotted-decimal format.
Cisco IOS XE Release 3.6S	This command was modified. The command output was enhanced to display route tag values in dotted-decimal format.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

### Usage Guidelines

The **show route-map** command displays information about route maps configured on the router. The output will vary depending on the keywords included with the command and the Cisco software image running on your router.

### Examples

The following is sample output from the **show route-map** command when no keywords or arguments are used:

```
Device# 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 sample output from the **show route-map** command displays information about route tags:

```

Device# show route-map

route-map STATIC, permit, sequence 10
  Match clauses:
    ip address (access-lists): 1
  Set clauses:
    metric 56 100 255 1 1500
    tag 1.1.1.1
  Policy routing matches: 0 packets, 0 bytes
route-map STATIC, permit, sequence 20
  Match clauses:
    ip address (access-lists): 2
  Set clauses:
    metric 56 100 255 1 1500
    tag 1.1.1.2
  Policy routing matches: 0 packets, 0 bytes

```

The following sample output from the **show route-map** command shows Multiprotocol Label Switching (MPLS)-related route map information:

```

Device# 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 following is sample output from the **show route-map dynamic** command:

```

Device# 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 dynamic application** command:

```
Device# show route-map dynamic application
```

```

Application - AAA
Number of active routemaps = 1

```

When you specify an application name, dynamic routes for that application are displayed. The following is sample output from the **show route-map dynamic application** command when you specify the name of the application:

```
Device# 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

```

```
Device# 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

```

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

```
Device# 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
```

The following is sample output from the **show route-map dynamic** command when a VRF is configured for VRF autotclassification:

```
Device# 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 vrf1
  Policy routing matches: 0 packets, 0 bytes
Current active dynamic routemaps = 1
```

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

**Table 35: show route-map Field Descriptions**

Field	Description
Route-map ROUTE-MAP-NAME	Name of the route map.
Permit	Indicates that the route is redistributed based on set actions.
Sequence	Number that indicates the position of the new route map in the list of configured route maps.
Match clauses	Match criteria or conditions based on which the route map is redistributed.
Continue	Displays the configuration of a continue clause and the next route-map entry to which the clause is sent.
Set clauses	Specific redistribution actions to be performed if the <b>match</b> command criteria are met.
Tag	Tag for routes to the remote network.
Policy routing matches	Number of packets and bytes that have been filtered by policy routing.

#### Related Commands

Command	Description
<b>redistribute (IP)</b>	Redistributes routes from one routing domain into another routing domain.
<b>route-map (IP)</b>	Defines conditions for redistributing routes from one routing protocol into another, or enables policy routing.
<b>match interface (IP)</b>	Distributes any route that has the next hop out of one of the specified interfaces.
<b>match ip next-hop</b>	Redistributes any route that has a next-hop router address that is passed by one of the specified access lists.
<b>match tag</b>	Filters routes that match specific route tags.

## show route-tag list

To display information about route tag lists configured on the router, use the **show route-tag list** command in user EXEC or privileged EXEC mode.

**show route-tag list** [*list-name*]

<b>Syntax Description</b>	<i>list-name</i>	Name of a specific route tag list.
---------------------------	------------------	------------------------------------

**Command Default** If this command is used without the *list-name* argument, information about all route tag lists configured on the router are displayed.

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	15.2(2)S	This command was introduced.
	Cisco IOS XE Release 3.6S	This command was integrated into Cisco IOS XE Release 3.6S.
	15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.

**Usage Guidelines** Use the *list-name* argument to display information about a specific route tag list. Route tags are 32-bit values attached to routes. They are used to filter routes. You can display route tag values as either plain decimals or dotted decimals. To enable **show** commands to display route tag values in dotted-decimal format, configure the **route-tag notation** command in global configuration mode.

### Examples

The following sample output from the **show route-tag list** command displays route tag information in dotted-decimal format. The fields in the display are self-explanatory.

```
Device# show route-tag list

route-tag-list List1 :
  permit 5 1.1.1.1 1.1.1.1
  permit 10 2.2.2.2 2.2.2.2
  permit 12 3.3.3.3 3.3.3.3
  permit 15 4.4.4.4 4.4.4.4
  permit 18 6.6.6.6 6.6.6.6
route-tag-list List2 :
  permit 5 1.1.1.1 1.1.1.1
  permit 10 2.2.2.2 2.2.2.2
  permit 12 3.3.3.3 3.3.3.3
  permit 15 4.4.4.4 4.4.4.4
  permit 18 6.6.6.6 6.6.6.6
```



**Related Commands**

<b>Command</b>	<b>Description</b>
<b>route-tag list</b>	Configures a route tag list.
<b>route-tag notation</b>	Enables the display of route tag values in dotted-decimal format.

## traffic-share min

To configure traffic to use minimum-cost routes, when there are multiple routes that have different-cost routes to the same destination network, use the **traffic-share min** command in router address family topology or router configuration mode. To disable this function, use the **no** form of this command.

**traffic-share min command**  
**traffic-share min across-interfaces**  
**no traffic-share min across-interfaces**

### Syntax Description

<b>across-interfaces</b>	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 <b>across-interfaces</b> 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-share min** 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-share min** command in router address family topology configuration mode in order for this OSPF router configuration command to become topology-aware.

### 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 the appropriate 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 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**

- Interface configuration (config-if)
- Pseudowire class configuration (config-pw-class)
- Template configuration (config-template)

Command History	Release	Modification
	15.0(1)S	This command was introduced.
	Cisco IOS XE Release 3.7S	This command was integrated into a release prior to Cisco IOS XE Release 3.7S. This command was modified as part of the MPLS-based Layer 2 VPN (L2VPN) command modifications for cross-OS support. This command was made available in interface configuration and template configuration modes in Cisco IOS XE Release 3.7S.

**Usage Guidelines** This command was modified as part of the MPLS-based Layer 2 VPN (L2VPN) command modifications for cross-OS support.

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. 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/UDP headers, then you must set the CC type to the CC Type 1 control word.

### Examples

The following example shows how to configure the MPLS pseudowire class to use CC Type 1:

```
Device(config)# pseudowire-class bfdclass
Device(config-pw-class)# encapsulation mpls
Device(config-pw-class)# protocol none
Device(config-pw-class)# vccv control-word
```

The following example shows how to configure the MPLS pseudowire class to use CC Type 1 in interface configuration mode:

```
Device(config)# interface pseudowire 100
Device(config-if)# encapsulation mpls
Device(config-if)# signaling protocol none
Device(config-if)# vccv control-word
```

The following example shows how to configure the MPLS pseudowire class to use CC Type 1 in template configuration mode:

```
Device(config)# template type pseudowire 100
Device(config-template)# encapsulation mpls
Device(config-template)# signaling protocol none
Device(config-template)# vccv control-word
```

#### Related Commands

Command	Description
<b>bfd-template</b>	Creates a BFD template and enters BFD configuration mode.
<b>encapsulation (pseudowire)</b>	Specifies an encapsulation type for tunneling Layer 2 traffic over a pseudowire.
<b>pseudowire-class</b>	Specifies the name of the pseudowire class and enters pseudowire class configuration mode.
<b>signaling protocol</b>	Specifies the signaling protocol to be used for signaling labels.
<b>vccv bfd template</b>	Enables VCCV BFD for a pseudowire class.
<b>vccv bfd status signaling</b>	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 **vccv bfd status signaling** command in the appropriate 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** Interface configuration (config-if)  
 Pseudowire class configuration (config-pw-class)  
 Template configuration (config-template)

Command History	Release	Modification
	15.0(1)S	This command was introduced.
	Cisco IOS XE Release 3.7S	This command was integrated into a release prior to Cisco IOS XE Release 3.7S. This command was modified as part of the Multiprotocol Label Switching (MPLS)-based L2VPN command modifications for cross-OS support. This command was made available in interface configuration and template configuration modes in Cisco IOS XE Release 3.7S.

**Usage Guidelines** Use this command to allow BFD to provide the status signaling functionality that indicates the fault status of an attachment circuit. This command is applicable only for static pseudowires; that is, when the signaling protocol is none.

### Examples

The following example shows how to enable VCCV BFD status signaling for a Multiprotocol Label Switching (MPLS) pseudowire class:

```
Device(config)# pseudowire-class bfdclass
Device(config-pw-class)# encapsulation mpls
Device(config-pw-class)# protocol none
Device(config-pw-class)# vccv control-word
Device(config-pw-class)# vccv bfd template bfdtemplate raw-bfd
Device(config-pw-class)# vccv bfd status signaling
```

The following example shows how to enable VCCV BFD status signaling in interface configuration mode:

```
Device(config)# interface pseudowire 100
Device(config-if)# encapsulation mpls
Device(config-if)# signaling protocol none
Device(config-if)# vccv control-word
```

```
Device(config-if)# vccv bfd template bfdtemplate raw-bfd
Device(config-if)# vccv bfd status signaling
```

The following example shows how to enable VCCV BFD status signaling in template configuration mode:

```
Device(config)# template type pseudowire 100
Device(config-template)# encapsulation mpls
Device(config-template)# signaling protocol none
Device(config-template)# vccv control-word
Device(config-template)# vccv bfd template bfdtemplate raw-bfd
Device(config-template)# vccv bfd status signaling
```

#### Related Commands

Command	Description
<b>bfd-template</b>	Creates a BFD template and enters BFD configuration mode.
<b>encapsulation (pseudowire)</b>	Specifies an encapsulation type for tunneling Layer 2 traffic over a pseudowire.
<b>pseudowire-class</b>	Specifies the name of the pseudowire class and enters pseudowire class configuration mode.
<b>signaling protocol</b>	Specifies the signaling protocol to be used for signaling labels.
<b>source template type pseudowire</b>	Configures the name of a source template of type pseudowire.
<b>vccv</b>	Configures the pseudowire VCCV CC type for MPLS pseudowires.
<b>vccv bfd template</b>	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 **vccv bfd template** command in the appropriate 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.
	<b>udp</b>	(Optional) Enables support for BFD with IP/UDP header encapsulation.
	<b>raw-bfd</b>	(Optional) Enables support for BFD without IP/UDP header encapsulation.

**Command Default** VCCV BFD is disabled for the pseudowire class. The template that is selected by default is raw-bfd.

**Command Modes**

- Interface configuration (config-if)
- Pseudowire class configuration (config-pw-class)
- Template configuration (config-template)

Command History	Release	Modification
	15.0(1)S	This command was introduced.
	Cisco IOS XE Release 3.7S	This command was integrated into a release prior to Cisco IOS XE Release 3.7S. The command was modified as part of the Multiprotocol Label Switching (MPLS)-based Layer 2 VPN (L2VPN) command modifications for cross-OS support. This command was made available in interface configuration and template configuration modes in Cisco IOS XE Release 3.7S.

**Usage Guidelines** Use the **bfd-template** command to specify the BFD template and settings for the BFD interval values. VCCV defines two types of 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.



**Note** IP/UDP is currently not supported.

**Examples**

The following example shows how to enable the BFD template without support for IP/UDP header encapsulation:

```
Device(config)# pseudowire-class bfdclass
Device(config-pw-class)# encapsulation mpls
Device(config-pw-class)# protocol none
Device(config-pw-class)# vccv control-word
Device(config-pw-class)# vccv bfd template bfdtemplate raw-bfd
Device(config-pw-class)# vccv bfd status signaling
```

The following example shows how to enable the BFD template without support for IP/UDP header encapsulation in interface configuration mode:

```
Device(config)# interface pseudowire 100
Device(config-if)# encapsulation mpls
Device(config-if)# Signaling protocol none
Device(config-if)# vccv control-word
Device(config-if)# vccv bfd template bfdtemplate raw-bfd
Device(config-if)# vccv bfd status signaling
```

The following example shows how to enable the BFD template without support for IP/UDP header encapsulation in template configuration mode:

```
Device(config)# template type pseudowire template1
Device(config-template)# encapsulation mpls
Device(config-template)# Signaling protocol none
Device(config-template)# vccv control-word
Device(config-template)# vccv bfd template bfdtemplate raw-bfd
Device(config-template)# vccv bfd status signaling
```

**Related Commands**

Command	Description
<b>bfd-template</b>	Creates a BFD template and enters BFD configuration mode.
<b>encapsulation (pseudowire)</b>	Specifies an encapsulation type for tunneling Layer 2 traffic over a pseudowire.
<b>pseudowire-class</b>	Specifies the name of the pseudowire class and enters pseudowire class configuration mode.
<b>signaling protocol</b>	Specifies the signaling protocol to be used for signaling labels.
<b>source template type pseudowire</b>	Configures the name of a source template of type pseudowire.
<b>vccv</b>	Configures the pseudowire VCCV CC type for MPLS pseudowires.
<b>vccv bfd template</b>	Enables VCCV BFD for a pseudowire class.