IP Routing Protocol-Independent Commands: S through T

send-lifetime

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

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

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

Syntax Description

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

Command Default

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

Command Modes

Key chain key configuration (config-keychain-key)

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

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

```
Router(config)# eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# network 10.0.0.0
Router(config-router-af)# af-interface ethernet0/0
```

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

Related Commands

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

set automatic-tag

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

Command	Description
set weight	Specifies the BGP weight for the routing table.
show route-map	Displays all route maps configured or only the one specified.

set default interface

To indicate where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination, use the **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

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

Command Default

This command is disabled by default.

Command Modes

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

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

set interface

To indicate where to forward packets that pass a match clause of a route map for policy routing, use the **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

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

Command Default

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

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
11.0	This command was introduced.
12.3(7)T	This command was 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 p1
!
access-list 101 permit ip 10.100.0.0 0.255.255.255 any
!
route-map test permit 10
 match ip address 101
 set interface Tunnel101
!
interface GigabitEthernet9/5
 description TO_CE_C1A_FastEther-5/5
 ip address 192.168.5.1 255.255.255.0
 ip policy route-map test
 no keepalive
```

Related Commands

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

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

set ip default next-hop

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

set ip default next-hop *ip-address* [*... ip-address*]

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

Syntax Description

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

Command Default

This command is disabled by default.

Command Modes

Route-map configuration

Command History

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

Usage Guidelines

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

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

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

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

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

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

Examples

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

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

Related Commands

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

Command	Description
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Indicates where to output packets that pass a match clause of route map for policy routing.
set ip next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing.

set ip default next-hop verify-availability

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

set ip default next-hop commandset ip default next-hop verify-availability

no set ip default next-hop verify-availability

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

Route-map configuration

Command History

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

Usage Guidelines

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

Examples

The following example:

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

Related Commands

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

set ip global

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

set ip global next-hop *ip-address* [*... ip-address*]

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

Syntax Description

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

Command Default

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

Command Modes

Route-map configuration

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

Command	Description
ip policy route-map	Identifies a route map to use for policy routing on an interface.

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

set ip next-hop

To indicate where to output packets that pass a match clause of a route map for policy routing, use the **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*]}

Syntax Description

ip-address	IP address of the next hop to which packets are output. It must be the address of an adjacent router.
dynamic dhcp	Dynamically sets the DHCP next hop.
encapsulate l3vpn	Sets the encapsulation profile for the L3VPN next hop.
profile-name	L3VPN encapsulation profile name.
peer-address	Sets the next hop as the Border Gateway Protocol peering address.
recursive *ip-address*	Sets the IP address of the recursive next-hop router. **Note** The next-hop IP address must be assigned separately from the recursive next-hop IP address.
global	(Optional) Sets the global routing table.
vrf *vrf-name*	(Optional) Sets the Virtual Routing and Forwarding instance.
verify-availability	Verifies if the next hop is reachable.
sequence	(Optional) The sequence to be inserted into the next-hop list. The range is from 1 to 65535.
track	(Optional) Sets the next hop depending on the state of a tracked object.
track-object-number	(Optional) The tracked object number. The range is from 1 to 500.

Command Default

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

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
11.0	This command was introduced.
12.0(28)S	This command was modified. The **recursive** keyword was added.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.2	In Cisco IOS XE Release 2.2, this command was integrated into the Cisco ASR 1000 Series Routers.
12.2(33)SRE	This command was modified. The **encapsulate** and **l3vpn** keywords were added.

Usage Guidelines

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

Use the **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
ip policy route-map	Identifies a route map to use for policy routing on an interface.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match length	Bases policy routing on the Level 3 length of a packet.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.

Command	Description
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Indicates where to output packets that pass a match clause of a route map for policy routing.
set ip default next-hop verify-availability	Indicates where to output packets that pass a match clause of a route map for policy routing and for which the Cisco IOS software has no explicit route to a destination.

set ip next-hop verify-availability

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

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

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

Syntax Description

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

Command Default

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

Command Modes

Route-map configuration (config-route-map)

Command History

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

Examples

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

```
! Configure the objects to be tracked.
! Object 123 will be up if the router can ping 10.1.1.1.
! Object 124 will be up if the router can ping 10.2.2.2.
ip sla monitor 1
 type echo protocol ipicmpecho 10.1.1.1
ip sla monitor schedule 1 start-time now life forever
!
ip sla monitor 2
 type echo protocol ipicmpecho 10.2.2.2
ip sla monitor schedule 2 start-time now life forever
!
track 123 rtr 1 reachability
track 124 rtr 2 reachability
!
! Enable policy routing using route-map alpha on Ethernet 0.
interface ethernet 0
 ip address 10.4.4.254 255.255.255.0
 ip policy route-map alpha
!
! 10.1.1.1 is via this interface
interface ethernet 1
 ip address 10.1.1.254 255.255.255.0
! 10.2.2.2 is via this interface
```

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

Related Commands

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

set ip vrf

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

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

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

Syntax Description

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

Command Default

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

Command Modes

Route-map configuration

Command History

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

Usage Guidelines

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

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

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

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

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

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

Examples

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

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

Related Commands

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

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

set level (IP)

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

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

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

Syntax Description

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

Command Default

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

Command Modes

Route-map configuration

Command History

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

Usage Guidelines

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

matchcriteria--the conditions under which redistribution is allowed for the current **route-map**command. The **set** commands specify the *setactions*--the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **noroute-map** command deletes the route map.

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

The **stub-areaandbackbonekeywordshavenoeffectonwhereroutesareimported.**

Examples

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

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

Related Commands

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

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

set local-preference

To specify a preference value for the autonomous system 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** form of this command.

set local-preference *number*

no set local-preference

Syntax Description

number	Preference value. An integer from 0 to 4294967295.

Command Default

Preference value of 100

Command Modes

Route-map configuration (config-route-map)

Command History

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

Usage Guidelines

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
```

Related Commands

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

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

set metric (BGP-OSPF-RIP)

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

set metric *metric-value*

no set metric *metric-value*

Syntax Description

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

Command Default

The dynamically learned metric value.

Command Modes

Route-map configuration (config-route-map)

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

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

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

set metric-type

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

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

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

Syntax Description

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

Command Default

This command is disabled by default.

Command Modes

Route-map configuration

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

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

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

set next-hop

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

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

no set next-hop *next-hop*

Syntax Description

next-hop	IP address of the next hop router.

Command Default

Default next hop address.

Command Modes

Route-map configuration

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

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

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

set tag (IP)

To set a tag value 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 *tag-value-dotted-decimal* argument was added to support tag values in dotted-decimal format.
Cisco IOS XE Release 3.6S	This command was modified. The *tag-value-dotted-decimal* argument was added to support tag values in dotted-decimal format.

Usage Guidelines

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
match tag	Filters routes that match specific route tags.
route-map (IP)	Defines conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set automatic-tag	Automatically computes the tag value.

set 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

vrf *vrf-name*	(Optional) Specifies explicitly that the default next-hops are under the specific Virtual Routing and Forwarding (VRF) instance.
global	(Optional) Specifies explicitly that the default next-hops are under the global routing table.
global-ipv6-address	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)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.
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
ipv6 local policy route-map	Identifies a route map to use for local IPv6 PBR.
ipv6 policy route-map	Configures IPv6 policy-based routing (PBR) on an interface.

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

set 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 [**vrf** *vrf-name*| **global**] **next-hop** *global-ipv6-address* [*global-ipv6-address...*]

no set ipv6 [**vrf** *vrf-name*| **global**] **next-hop** *global-ipv6-address* [*global-ipv6-address...*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies explicitly that next-hops are under the specific Virtual Routing and Forwarding (VRF) instance.
global	(Optional) Specifies explicitly that next-hops are under the global routing table.
global-ipv6-address [*global-ipv6-address...*]	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)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

The following **set** commands support inherit-VRF, inter-VRF, and VRF-to-global routing in an IPv6-specific implementation:

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 *global-ipv6-address* argument. A global IPv6 address must be specified. An IPv6 link-local address cannot be used because the use of an IPv6 link-local address requires interface context.

The *global-ipv6-address* argument must specify an address that is installed in the IPv6 Routing Information Base (RIB) and is directly connected. A directly connected address is an address that 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 the packet is 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
ipv6 local policy route-map	Identifies a route map to use for local IPv6 PBR.
ipv6 policy route-map	Configures IPv6 PBR on an interface.
match ipv6 address	Specifies an IPv6 access list to use to match packets for PBR for IPv6.
match length	Bases policy routing on the Level 3 length of a packet.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Indicates where to output packets that pass a match clause of a route map for policy routing.
set ipv6 default next-hop	Specifies an IPv6 default next hop to which matching packets are forwarded.
set ipv6 precedence	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

precedence-value	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)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

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

set 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

vrf-name	Name of the VRF instance.
next-hop-address	IP address of the next hop to which packets will be forwarded.
sequence	Sequence of next hops. The range is from 1 to 65535.
track	Specifies the tracking method.
object	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.

Examples

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
show route-map	Displays the configured route maps.
track	Tracks the state of an interface, an ip route, or a response time reporter.

show dampening interface

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

show dampening interface commandshow dampening interface

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC Privileged EXEC

Command History

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

Examples

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

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

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

Table 1: 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.

Related Commands

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

show 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)SXI4	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

interface *type number*	Specified interface for which PBR VMR information will be displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXI4	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 **showinterface** dampening command in privileged EXEC mode.

show interface dampening commandshow interface dampening

Syntax Description

This command has no keywords or arguments.

Command Modes

Privileged EXEC

Command History

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

Examples

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

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

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

Table 2: 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.

Field	Description
HalfL	Displays the half-life counter.
ReuseV	Displays the reuse threshold timer.
SuppV	Displays the suppress threshold.
MaxSTm	Displays the maximum suppress.
MaxP	Displays the maximum penalty.
Restart	Displays the restart timer.

Related Commands

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

show ip cef platform

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

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

Syntax Description

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

Command Modes

Privileged EXEC (#)

Command History

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

Examples

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

```
Router# show ip cef 10.4.4.4 platform

10.4.4.4/32
Fib Entry: 0xD6680610 XCM leaf from 0x50805550(RP) 0xA0805550(FP):
load_bal_or_adj[0] 0x0 load_bal_or_adj[1] 0x18 load_bal_or_adj[2] 0x1C
leaf points to an adjacency, index 0x607
ip_mask 0x0 as_number 0x0 precedence_num_loadbal_intf 0xF0 qos_group 0x0
Label object OCE Chain:
Label(0x12, real) Adjacency
c10k_label_data = 0x450467F8
tag_elt_addr = 0x50003038
ipv6_tag_elt_addr = 0x0
tag_index = 0x607
tt_tag_rew = 0x45046800
Tag Rewrite: vcci = 0x9DA, fib_root = 0x0
mac_rewrite_index = 0x395, flags = 0x9
pktswitched = 0 byteswitched = 0
XCM Tag Rewrite: vcci = 0x9DA, fib_root = 0x0
```

```
mac_rewrite_index = 0x395, flags = 0x9
mac_index_extension = 0x0
XCM mac rewrite from index 0x395
mtu from 0x53800E54(RP) 0xA3800E54(FP)
frag_flags = 0x0
mtu = 1496
mac length 0x12 encap length 0x16 upd_offset=0x02FF
mac string start from bank4 0x32001CA8(RP)
0x82001CA8(FP)
mac string end from bank9 0x50801CA8(RP)
0xA0801CA8(FP)
Encap String: 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
show cef	Displays which packets the line cards dropped, or displays which packets were not express forwarded.
show cef interface	Displays Cisco Express Forwarding-related interface information.

show ip static route bfd

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

show ip static route bfd [*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

interface-type interface-number	(Optional) Interface type and interface number for which BFD is configured.
destination-ip-address	(Optional) Multihop BFD destination IP address or the gateway IP address.
group *group-name*	(Optional) Specifies a BFD group and group name.
vrf	(Optional) Specifies the Virtual Routing and Forwarding (VRF) instance.
destination-vrf-name	(Optional) Destination VRF name.
source-vrf-name	(Optional) Source VRF name.
source-ip-address	(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 **vrf** keyword, and *interface-type*, *interface-number*, *destination-ip-address*, *source-ip-address*, *destination-vrf-name*, and *source-vrf-name* 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.

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 3: 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
ip route static bfd	Specifies static route BFD neighbors.
show ip static route	Displays static route database information.

show ip cache policy

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

show ip cache policy commandshow ip cache policy

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

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

Examples

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

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

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

Table 4: show ip cache policy Field Descriptions

Field	Description
Total adds	Number of times a cache entry was created.
total deletes	Number of times a cache entry or the entire cache was deleted.
Type	“NH” indicates the **setipnext-hop** command. “Int” indicates the **setinterface**command.
Routemap	Name of the route map that created the entry; in this example, george.
sequence	Route map sequence number.

Field	Description
Age	Age of the cache entry.
Interface	Output interface type and number.
Next Hop	IP address of the next hop.

Related Commands

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

show ip local policy

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

show ip local policy commandshow ip local policy

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

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

Examples

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

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

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

Table 5: 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.

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

Related Commands

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

show ip policy

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

show ip policy

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
11.1	This command was introduced.
12.3(7)T	The display output was modified to include a label for dynamic route maps.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

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 6: show ip policy Field Descriptions

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

Related Commands

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

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

show ip protocols

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

show ip protocols commandshow ip protocols

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.2(15)T	This command was modified. Support for the route-hold timer was integrated into the output.
12.2(28)SB	This command was integrated into Cisco IOS 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(2)S	This command was modified. The output of the command was modified to display that Routing Information Protocol (RIP) default routes are sent on passive interfaces.

Usage Guidelines

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

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

Examples

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

```
Router# show ip protocols
*** IP Routing is NSF aware ***
Routing Protocol is "eigrp 3"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Default networks flagged in outgoing updates
```

```
Default networks accepted from incoming updates
Redistributing: eigrp 3
EIGRP-IPv4 VR(test) Address-Family Protocol for AS(3)
Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
NSF-aware route hold timer is 240
Router-ID: 10.1.1.1
Topology : 0 (base)
Active Timer: 3 min
Distance: internal 90 external 170
Maximum path: 4
Maximum hopcount 100
Maximum metric variance 1
Total Prefix Count: 3
Total Redist Count: 0
Automatic Summarization: disabled
Maximum path: 4
Routing for Networks:
10.0.0.0
Routing Information Sources:
Gateway Distance Last Update
10.1.1.2 90 00:05:10
Distance: internal 90 external 170
```

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

Table 7: show ip protocols Field Descriptions

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

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

Examples

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

```
Router# show ip protocols
Routing Protocol is “isis”
  Sending updates every 0 seconds
  Invalid after 0 seconds, hold down 0, flushed after 0
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Redistributing: isis
  Address Summarization:
    None
  Routing for Networks:
    Serial0
  Routing Information Sources:
  Distance: (default is 115)
```

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

Table 8: show ip protocols Field Descriptions for an IS-IS Process

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

Examples

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

```
Router# show ip protocols
Routing Protocol is "rip"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Sending updates every 30 seconds, next due in 6 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Sending Default route on Passive interfaces
  Redistributing: rip
  Default version control: send version 2, receive version 2
  Automatic network summarization is not in effect
```

```
  Maximum path: 4
  Routing for Networks:
    172.19.0.0
    10.2.0.0
    10.3.0.0
  Passive Interface(s):
    Ethernet0/0
    Ethernet0/1
    Ethernet0/2
    Ethernet0/3
    Ethernet1/0
    Ethernet1/1
    Ethernet1/2
    Ethernet1/3
  Passive Interface(s):
    Serial2/0
    Serial2/1
    Serial2/2
    Serial2/3
    Serial3/0
    Serial3/1
    Serial3/2
    Serial3/3
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: (default is 120)
```

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

Table 9: 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.

Field	Description
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: • IP address • Administrative distance • Time the last update was received from this source

Examples

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

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

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

Table 10: 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.

Field	Description
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: • IP address • Administrative distance • Time the last update was received from this source

Related Commands

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

show ip route

To display 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

ip-address	(Optional) IP address for which routing information should be displayed.
repair-paths	(Optional) Displays the repair paths.
next-hop-override	(Optional) Displays the Next Hop Resolution Protocol (NHRP) next-hop overrides that are associated with a particular route and the corresponding default next hops.
dhcp	(Optional) Displays routes added by the Dynamic Host Configuration Protocol (DHCP) server.
mask	(Optional) Subnet mask.
longer-prefixes	(Optional) Displays output for longer prefix entries.
protocol	(Optional) The name of a routing protocol or the keyword **connected**, **mobile**, **static**, or **summary**. If you specify a routing protocol, use one of the following keywords: **bgp**, **eigrp**, **hello**, **isis**, **odr**, **ospf**, **nhrp**, or **rip**.
process-id	(Optional) Number used to identify a process of the specified protocol.
list	(Optional) Filters output by an access list name or number.
access-list-number	(Optional) Access list number.
access-list-name	(Optional) Access list name.
static	(Optional) Displays static routes.
download	(Optional) Displays routes installed using the authentication, authorization, and accounting (AAA) route download function. This keyword is used only when AAA is configured.

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

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
9.2	This command was introduced.
10.0	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 *process-id* argument was added.
11.0	This command was modified. The **longer-prefixes** 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 **update-queue** 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.

Release	Modification
12.2(13)T	This command was modified. The *egp* and *igrp* 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.
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 **dhcp** and **repair-paths** 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 **next-hop-override** and **nhrp** 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.

Examples

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 10.0.0.0/8 is subnetted, 3 subnets
P       10.1.1.0 [200/0] via 172.31.229.41, Dialer1
P       10.1.3.0 [200/0] via 172.31.229.41, Dialer1
P       10.1.2.0 [200/0] via 172.31.229.41, Dialer1

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 remote1
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
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
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 11: show ip route Field Descriptions

Field	Description
Codes (Protocol)	Indicates the protocol that derived the route. It can be one of the following values: • B—BGP derived • C—Connected • D—Enhanced Interior Gateway Routing Protocol (EIGRP) • EX—EIGRP external • H—NHRP • i—IS-IS derived • ia—IS-IS • L—Local • M—Mobile • o—On-demand routing • O—Open Shortest Path First (OSPF) derived • P—Periodic downloaded static route • R—Routing Information Protocol (RIP) derived • S—Static • U—Per-user static route • +—Replicated route
Codes (Type)	Type of route. It can be one of the following values: • *—Indicates the last path used when a packet was forwarded. This information is specific to nonfast-switched packets. • E1—OSPF external type 1 route • E2—OSPF external type 2 route • IA—OSPF interarea route • L1—IS-IS Level 1 route • L2—IS-IS Level 2 route • N1—OSPF not-so-stubby area (NSSA) external type 1 route • N2—OSPF NSSA external type 2 route

Field	Description
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.

Examples

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 12: 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.

Field	Description
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
```

Examples

The following example shows that IP route 10.8.8.0 is directly connected to the Internet and is the next-hop (option 3) default gateway. Routes 10.1.1.1 [1/0], 10.3.2.1 [24/0], and 172.16.2.2 [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

Command	Description
show interfaces tunnel	Displays tunnel interface information.
show ip route summary	Displays the current state of the routing table in summary format.

show ip route loops

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

show ip route loops

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

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

Usage Guidelines

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

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

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

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

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

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

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

Examples

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

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

Related Commands

Command	Description
ip route	Establishes static routes.

show ip route profile

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

sshow ip route profile commandhow ip route profile

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

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

Usage Guidelines

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

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 13: show ip route profile Field Descriptions

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

Related Commands

Command	Description
ip route profile	Enables IP routing table statistics collection

show ip route summary

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

shshow ip route summary commandow ip route summary

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

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

Examples

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

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

show ip route summary describes the significant fields shown in the display.

Table 14: 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.

Field	Description
Route Source	Routing protocol name, or the **connected,static,** or **internal**keyword. “Internal” indicates those routes that are in the routing table that are not owned by any routing protocol.
Networks	Number of prefixes that are present in the routing table for each route source.
Subnets	Number of subnets that are present in the routing table for each route source, including host routes.
Overhead	Any additional memory involved in allocating the routes for the particular route source other than the memory specified in the Memory field.
Memory	Number of bytes allocated to maintain all the routes for the particular route source.

show ip route supernets-only

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

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

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

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

Examples

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

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

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

Table 15: 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).

Field	Description
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

tag-value	Route tag value in plain decimals. The range is from 1 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.
mask	(Optional) Route tag wildcard mask.

Command Modes

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.

```
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 16: 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.

Field	Description
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.
Loading	Displays the total load on the link.
Route tag	Displays the tag of the prefix or network.

Related Commands

Command	Description
show ipv6 route tags	Displays route tag entries for IPv6 routes.

show ip route track-table

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

show ip route track-table

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

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

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 17: show ip route track-table Field Descriptions

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

Related Commands

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

show ip 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

vrf-name	Name of the VRF.
connected	(Optional) Displays all connected routes in a VRF.
protocol	(Optional) Routing protocol. To specify a routing protocol, use one of the following keywords: **bgp**, **egp**, **eigrp**, **hello**, **igrp**, **isis**, **ospf**, or **rip**.
as-number	(Optional) Autonomous system number.
list *number*	(Optional) Specifies the IP access list to be displayed.
profile	(Optional) Displays the IP routing table profile.
static	(Optional) Displays static routes.
summary	(Optional) Displays a summary of routes.
ip-prefix	(Optional) Network for which routing information is displayed.
ip-address	(Optional) Address for which routing information is displayed.
mask	(Optional) Network mask.
longer-prefixes	(Optional) Displays longer prefix entries.
repair-paths	(Optional) Displays repair paths.
dhcp	(Optional) Displays routes added by the DHCP server.
supernets-only	(Optional) Displays only supernet entries.
tag	(Optional) Displays information about route tags in the VRF table.
tag-value	(Optional) Route tag values as a plain decimals.

tag-value-dotted-decimal	(Optional) Route tag values as a dotted decimals.
mask	(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 *ip-prefix* 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 **repair-paths**, **dhcp**, and **supernets-only** 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 **tag** keyword and *tag-value*, *tag-value-dotted-decimal*, and *mask* 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 **tag** keyword and *tag-value*, *tag-value-dotted-decimal*, and *mask* 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.

Release	Modification
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

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 18: 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).

Field	Description
Routing Descriptor Blocks	Displays the next-hop IP address followed by the information source.
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 19: show ip route vrf Field Descriptions

Field	Description
MPLS label	Displays the BGP prefix from the BGP peer. The output shows one of the following values: • A label value (16–1048575). • A reserved label value, such as explicit-null or implicit-null. • The word "none" if no label is received from the peer. The MPLS label field is not displayed if any of the following conditions is true: • BGP is not the Label Distribution Protocol (LDP). However, Open Shortest Path First (OSPF) prefixes learned via sham links display an MPLS label. • MPLS is not supported. • 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.
MPLS Flags	Name of the MPLS flag. One of the following MPLS flags is displayed: • MPLS Required—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. • No Global—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. • NSF—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.

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
```

Related Commands

Command	Description
show ip cache	Displays the Cisco Express Forwarding table associated with a VRF.
show ip vrf	Displays the set of defined VRFs and associated interfaces.

show ip static route

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

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

Syntax Description

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

Command Modes

User EXEC Privileged EXEC

Command History

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

Examples

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

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

```
       DN - Default Network, T - Tracking object
       L - TL1, E - OER
Codes in []: A - active, N - non-active, B - BFD-tracked, P - permanent
```

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

Table 20: 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

interface-type interface-number	(Optional) Interface type and interface number for which BFD is configured.
destination-ip-address	(Optional) Multihop BFD destination IP address or the gateway IP address.
group *group-name*	(Optional) Specifies a BFD group and group name.
vrf	(Optional) Specifies the Virtual Routing and Forwarding (VRF) instance.
destination-vrf-name	(Optional) Destination VRF name.
source-vrf-name	(Optional) Source VRF name.
source-ip-address	(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 **vrf** keyword, and *interface-type*, *interface-number*, *destination-ip-address*, *source-ip-address*, *destination-vrf-name*, and *source-vrf-name* 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.

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 21: 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
ip route static bfd	Specifies static route BFD neighbors.
show ip static route	Displays static route database information.

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)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

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
show route-map	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

ipv6-address	(Optional) Displays routing information for a specific IPv6 address.
ipv6-prefix	(Optional) Displays routing information for a specific IPv6 network.
/*prefix-length*	(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.
longer-prefixes	(Optional) Displays output for longer prefix entries.
protocol	(Optional) The name of a routing protocol or the keyword **connected**, **local**, **mobile**, or **static**. If you specify a routing protocol, use one of the following keywords: **bgp**, **isis**, **eigrp**, **ospf**, or **rip**.
repair	(Optional) Displays routes with repair paths.
updated	(Optional) Displays routes with time stamps.
boot-up	(Optional) Displays routing information since bootup.
day month	(Optional) Displays routes since the specified day and month.
time	(Optional) Displays routes since the specified time, in *hh:mm* format.
interface	(Optional) Displays information about the interface.
type	(Optional) Interface type.
number	(Optional) Interface number.
nd	(Optional) Displays only routes from the IPv6 Routing Information Base (RIB) that are owned by Neighbor Discovery (ND).

nsf	(Optional) Displays routes in the nonstop forwarding (NSF) state.
repair	(Optional)
table *table-id*	(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.
watch	(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 **isis** 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 **longer-prefixes** 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.

Release	Modification
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 **table**, **nsf**, **watch**, and **updated** keywords and the *day, month, table-id*, and *time* 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 **nd** 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 22: show ipv6 route Field Descriptions

Field	Description
Codes:	Indicates the protocol that derived the route. Values are as follows: • B—BGP derived • C—Connected • I1—ISIS L1—Integrated IS-IS Level 1 derived • I2—ISIS L2—Integrated IS-IS Level 2 derived • IA—ISIS interarea—Integrated IS-IS interarea derived • L—Local • R—RIP derived • S—Static
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

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
ipv6 route	Establishes a static IPv6 route.
show ipv6 interface	Displays IPv6 interface information.
show ipv6 route summary	Displays the current contents of the IPv6 routing table in summary format.
show ipv6 tunnel	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 23: show ipv6 route shortcut Field Descriptions

Field	Description
Codes:	Indicates the protocol that derived the route. Values are as follows: • C--Connected • L--Local • S--Static • R--RIP derived • B--BGP derived • I1--ISIS L1--Integrated IS-IS Level 1 derived • I2--ISIS L2--Integrated IS-IS Level 2 derived • IA--ISIS interarea--Integrated IS-IS interarea derived
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
ipv6 route	Establishes a static IPv6 route.
show ipv6 interface	Displays IPv6 interface information.
show ipv6 route summary	Displays the current contents of the IPv6 routing table in summary format.
show ipv6 tunnel	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 24: show ipv6 route summary Field Descriptions

Field	Description
entries	Number of entries in the IPv6 routing table.

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
show ipv6 route	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

tag-value	Route tag value in plain decimals. The range is from 1 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.
mask	(Optional) Route tag wildcard mask.

Command Modes

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.

```
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 25: show ipv6 route tag Field Descriptions

Field	Description
Codes	Indicates the protocol that derived the route. It can be one of the following values: • B—BGP derived • C—Connected • D—Enhanced Interior Gateway Routing Protocol (EIGRP) • EX—EIGRP external • H—NHRP • i—IS-IS derived • L—Local • O—Open Shortest Path First (OSPF) derived • P—Periodic downloaded static route • R—Routing Information Protocol (RIP) derived • S—Static • U—Per-user static route
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.

Field	Description
Ethernet0/0	Specifies the interface through which the specified network can be reached.

Related Commands

Command	Description
show ip route tag	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

vrf-name	Name assigned to the VRF.
vrf-number	Hexadecimal number assigned to the VRF.
tag	(Optional) Displays information about route tags in the VRF table.
tag-value	(Optional) Displays route tag value in plain decimals.
tag-value-dotted-decimal	(Optional) Displays route tag values in dotted decimals.
mask	(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 **tag** keyword and the *tag-value*, *tag-value-dotted-decimal*, and *mask* 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 **tag** keyword and the *tag-value*, *tag-value-dotted-decimal*, and *mask* 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.

Release	Modification
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

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 26: show ipv6 route vrf Field Descriptions

Field	Description
Codes	Indicates the protocol that derived the route. It can be one of the following values: • B—BGP derived • C—Connected • D—Enhanced Interior Gateway Routing Protocol (EIGRP) • EX—EIGRP external • H—NHRP • I—IS-IS derived • L—Local • O—Open Shortest Path First (OSPF) derived • P—Periodic downloaded static route • R—Routing Information Protocol (RIP) derived • S—Static • U—Per-user static route
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

interfaces	Displays information about platform support capability for all interfaces running IS-IS.
type	(Optional) Interface type. For more information, use the question mark (?) online help function.
number	(Optional) Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
summary	Displays FRR configuration information summary.
remote-lfa tunnels	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 **remote-lfa tunnels** 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 27: 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 28: 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
debug isis fast-reroute	Enables debugging of IS-IS FRR.
fast-reroute load-sharing	Disables FRR load sharing of prefixes.
fast-reroute per-prefix	Enables FRR per prefix.
fast-reroute tie-break	Configures the FRR tiebreaking priority.

show key chain

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

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

Syntax Description

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

Command Default

Information about all key chains is displayed.

Command Modes

EXEC

Command History

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

Examples

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

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

Related Commands

Command	Description
accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.
key	Identifies an authentication key on a key chain.
key chain	Enables authentication for routing protocols.

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

show monitor event-trace

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

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

Syntax Description

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

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

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

The trace function is not locked while information is being displayed to the console, which means that new trace messages can accumulate in memory. If entries accumulate faster than they can be displayed, some messages can be lost. If this happens, the **showmonitorevent-trace** command will generate a message indicating that some messages might be lost; however, messages will continue to display on the console. If the number of lost messages is excessive, the **showmonitorevent-trace**command will stop displaying messages.

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

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

Examples

Examples

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

```
Router# show monitor event-trace ipc

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

Examples

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

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

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

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

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

Examples

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

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

```
     spa type 0x0, fail code 0x0(none)
00:02:02.308: subslot 2/1: not present, TSM Event:remove_complete  New state:idle
00:02:02.308: subslot 2/2: not present, TSM Event:empty  New state:remove
     spa type 0x0, fail code 0x0(none)
00:02:02.308: subslot 2/2: not present, TSM Event:remove_complete  New state:idle
00:02:02.312: subslot 2/3: not present(plugin 4xOC3 POS SPA), TSM Event:empty  New
state:remove
     spa type 0x0, fail code 0x0(none)
00:02:02.312: subslot 2/3: not present, TSM Event:remove_complete  New state:idle
```

Examples

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

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

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

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

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

The following example shows Cisco Express Forwarding interface events:

```
Router# show monitor event-trace cef interface all
00:00:24.624: <empty>      (sw  4) Create   new
00:00:24.624: <empty>      (sw  4) SWIDBLnk FastEthernet0/0(4)
00:00:24.624: Fa0/0        (sw  4) NameSet
00:00:24.624: <empty>      (hw  1) Create   new
00:00:24.624: <empty>      (hw  1) HWIDBLnk FastEthernet0/0(1)
00:00:24.624: Fa0/0        (hw  1) NameSet
00:00:24.624: <empty>      (sw  3) Create   new
00:00:24.624: <empty>      (sw  3) SWIDBLnk FastEthernet0/1(3)
00:00:24.624: Fa0/1        (sw  3) NameSet
00:00:24.624: <empty>      (hw  2) Create   new
```

Examples

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

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

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

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

The following examples show Cisco Express Forwarding interface events:

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

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

Examples

To troubleshoot errors in an encryption datapath, enter the

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

```
Router# show monitor event-trace cfd all
00:00:42.452: 450000B4 00060000 FF33B306 02020203 02020204 32040000 F672999C
        00000001 7A7690C2 A0A4F8BC E732985C D6FFDCC8 00000001 C0902BD0
        A99127AE 8EAA22D4
00:00:44.452: 450000B4 00070000 FF33B305 02020203 02020204 32040000 F672999C
        00000002 93C01218 2325B697 3C384CF1 D6FFDCC8 00000002 BFA13E8A
        D21053ED 0F62AB0E
00:00:46.452: 450000B4 00080000 FF33B304 02020203 02020204 32040000 F672999C
        00000003 7D2E11B7 A0BA4110 CC62F91E D6FFDCC8 00000003 7236B930
        3240CA8C 9EBB44FF
00:00:48.452: 450000B4 00090000 FF33B303 02020203 02020204 32040000 F672999C
        00000004 FB6C80D9 1AADF938 CDE57ABA D6FFDCC8 00000004 E10D8028
```

```
        6BBD748F 87F5E253
00:00:50.452: 450000B4 000A0000 FF33B302 02020203 02020204 32040000 F672999C
        00000005 697C8D9D 35A8799A 2A67E97B D6FFDCC8 00000005 BC21669D
        98B29FFF F32670F6
00:00:52.452: 450000B4 000B0000 FF33B301 02020203 02020204 32040000 F672999C
        00000006 CA18CBC4 0F387FE0 9095C27C D6FFDCC8 00000006 87A54811
        AE3A0517 F8AC4E64
```

Related Commands

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

show platform hardware qfp active feature cef-mpls prefix ip

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

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

Syntax Description

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

Command Modes

Privileged EXEC (#)

Command History

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

Examples

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

```
Router# show platform hardware qfp active feature cef-mpls prefix ip 0.0.0.0/1 vrf
Gtrie Node Type: Leaf Node
HW Content: : 00002000 00000000 897daf40 895db490
  QPPB QoS Precedence valid: 0
  QoS Precedence: 0
  QPPB QoS Group valid: 0
  QoS Group: 0
  BGPPA Traffic Index valid: 0
  BGPPA Traffic Index: 0
  TBLF refcount: 2
  TBLF application lf handle: 0
```

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

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

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

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

show platform hardware qfp active feature cef-mpls prefix ipv6

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

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

Syntax Description

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

Command Modes

Privileged EXEC (#)

Command History

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

Examples

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

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

=== Gtrie Node ===

Gtrie Node Type: Tree Node
HW Content: : 89d000cd 00000004 60000000 00000000
Gtrie Tree Node Type:: Search Trie Node
=== Gtrie Search Node ===
  TN type 0, TN scan use 0, TN stride 6
  TN inode exists 1, TN skip 0
  TN zero perf real len: 0
```

```
  TN par bl offset: 0
  TN par bl len: 0
TBM Tree Array
  TA NNodes 2, TA INode Exists 1, TN TNRefs 0x11608698
TBM Tree Node Bitmap
Search Node Bitmap: 60 00 00 00 00 00 00 00
=== Gtrie Node ===

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

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

show platform hardware qfp active feature cef-mpls prefix mpls

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

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

Syntax Description

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

Command Modes

Privileged EXEC (#)

Command History

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

Examples

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

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

=== Gtrie Node ===

Gtrie Node Type: Tree Node
HW Content: : 89b00cad 00000000 80000000 00000000
Gtrie Tree Node Type:: Search Trie Node
=== Gtrie Search Node ===
  TN type 0, TN scan use 0, TN stride 6
  TN inode exists 0, TN skip 0
  TN zero perf real len: 0
  TN par bl offset: 0
  TN par bl len: 0
TBM Tree Array
```

```
  TA NNodes 1, TA INode Exists 0, TN TNRefs 0x116085e8
TBM Tree Node Bitmap
Search Node Bitmap: 80 00 00 00 00 00 00 00
=== Gtrie Node ===

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

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

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

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

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

show route-map

To display static and dynamic route maps 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

map-name	(Optional) Name of a specific route map.
dynamic	(Optional) Displays dynamic route map information.
dynamic-map-name	(Optional) Name of a specific, dynamic route map.
application	(Optional) Displays dynamic route maps based on applications.
application-name	(Optional) Name of a specific application.
all	(Optional) Displays all static and dynamic route maps.
detailed	(Optional) Displays 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.

Release	Modification
12.3(7)T	This command was modified. The **dynamic**, **application**, and **all** keywords were added.
12.0(28)S	This command was modified. Support for the recursive next-hop clause was added to the command output.
12.3(14)T	This command was modified. Support for the recursive next-hop clause, map display extension functionality, and the **detailed** 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 **detailed** 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

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 autoclassification:

```
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 29: 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 **match** 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
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.
route-map (IP)	Defines conditions for redistributing routes from one routing protocol into another, or enables policy routing.
match interface (IP)	Distributes any route that has the next hop out of one of the specified interfaces.
match ip next-hop	Redistributes any route that has a next-hop router address that is passed by one of the specified access lists.
match tag	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*]

Syntax Description

list-name	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 (#)

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 *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

Command	Description
route-tag list	Configures a route tag list.
route-tag notation	Enables the display of route tag values in dotted-decimal format.

traffic-share min

To c onfigure traffic to use minimum-cost routes, when there are multiple routes that have different-cost routes to the same destination network, use the**traffic-sharemin**command in router address family topology or router configuration mode. To disable this function, use the **no** form of this command.

traffic-share min commandtraffic-share min across-interfaces

no traffic-share min across-interfaces

Syntax Description

across-interfaces	Configures multi-interface load splitting on several interfaces with equal-cost paths.

Command Default

Traffic is configured to use minimum-cost paths.

Command Modes

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

Command History

Release	Modification
10.0	This command was introduced.
11.0(3)	This command became protocol independent when the **across-interfaces**keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was made available in router address family topology configuration mode.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **traffic-sharemin** command causes the Cisco IOS software to divide traffic only among the routes with the best metric. Other routes will remain in the routing table, but will receive no traffic. Configuring this command with the **across-interfaces** keyword allows you to configure multi-interface load splitting on different interfaces with equal-cost paths.

Release 12.2(33)SRB

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

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
bfd-template	Creates a BFD template and enters BFD configuration mode.
encapsulation (pseudowire)	Specifies an encapsulation type for tunneling Layer 2 traffic over a pseudowire.
pseudowire-class	Specifies the name of the pseudowire class and enters pseudowire class configuration mode.
signaling protocol	Specifies the signaling protocol to be used for signaling labels.
vccv bfd template	Enables VCCV BFD for a pseudowire class.
vccv bfd status signaling	Enables status signaling for BFD VCCV.

vccv bfd status signaling

To enable status signaling for Bidirectional Forwarding Detection (BFD) Virtual Circuit Connection Verification (VCCV), use the **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
bfd-template	Creates a BFD template and enters BFD configuration mode.
encapsulation (pseudowire)	Specifies an encapsulation type for tunneling Layer 2 traffic over a pseudowire.
pseudowire-class	Specifies the name of the pseudowire class and enters pseudowire class configuration mode.
signaling protocol	Specifies the signaling protocol to be used for signaling labels.
source template type pseudowire	Configures the name of a source template of type pseudowire.
vccv	Configures the pseudowire VCCV CC type for MPLS pseudowires.
vccv bfd template	Enables VCCV BFD for a pseudowire class.

vccv bfd template

To enable Virtual Circuit Connection Verification (VCCV) Bidirectional Forwarding Detection (BFD) for a pseudowire class, use the **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.
udp	(Optional) Enables support for BFD with IP/UDP header encapsulation.
raw-bfd	(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
bfd-template	Creates a BFD template and enters BFD configuration mode.
encapsulation (pseudowire)	Specifies an encapsulation type for tunneling Layer 2 traffic over a pseudowire.
pseudowire-class	Specifies the name of the pseudowire class and enters pseudowire class configuration mode.
signaling protocol	Specifies the signaling protocol to be used for signaling labels.
source template type pseudowire	Configures the name of a source template of type pseudowire.

Command	Description
vccv	Configures the pseudowire VCCV CC type for MPLS pseudowires.
vccv bfd template	Enables VCCV BFD for a pseudowire class.