

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

<i>start-time</i>	Beginning time that the key specified by the key command is valid to be sent. The syntax can be either of the following: <i>hh:mm:ss Month date year</i> <i>hh:mm:ss date Month year</i> <i>hh</i> —hours <i>mm</i> —minutes <i>ss</i> —seconds <i>Month</i> —first three letters of the month <i>date</i> —date (1–31) <i>year</i> —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 <i>start-time</i> value on.
<i>end-time</i>	Key is valid to be sent from the <i>start-time</i> value until the <i>end-time</i> value. The syntax is the same as that for the <i>start-time</i> value. The <i>end-time</i> value must be after the <i>start-time</i> value. The default end time is an infinite time period.
duration <i>seconds</i>	Length of time (in seconds) that the key is valid to be sent.

Defaults

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

Command Modes

Key chain key configuration

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 called 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 discrepancies in the set time of the router. There is a 30-minute leeway on each side to handle time differences.

```
interface ethernet 0
 ip rip authentication key-chain chain1
 ip rip authentication mode md5
!
router rip
 network 172.19.0.0
 version 2
!
key chain chain1
 key 1
 key-string key1
 accept-lifetime 13:30:00 Jan 25 1996 duration 7200
 send-lifetime 14:00:00 Jan 25 1996 duration 3600
 key 2
 key-string key2
 accept-lifetime 14:30:00 Jan 25 1996 duration 7200
 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	Enables 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.

Defaults 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** 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 configures the Cisco IOS software to automatically compute the tag value for the Border Gateway Protocol (BGP) learned routes:

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

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

set default interface

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

```
set default interface type number [...type number]
```

```
no set default interface type number [...type number]
```

Syntax Description

<i>type</i>	Interface type, used with the interface number, to which packets are output.
<i>number</i>	Interface number, used with the interface type, to which packets are output.

Command Default

This command is disabled by default.

Command Modes

Route-map configuration

Command History

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

Usage Guidelines

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

Use this command to provide certain users a different default route. If the Cisco IOS software has no explicit route for the destination, then it routes the packet to this interface. The first interface specified with the **set default interface** command that is up 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 policy route-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	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 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

<i>type</i>	Interface type, used with the interface number, to which packets are forwarded.
<i>number</i>	Interface number, used with the interface type, to which packets are forwarded.

Command Default

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

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
11.0	This command was introduced.
12.3(7)T	This command was 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.

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 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
```

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

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

In the following example, a TE tunnel interface is configured on a Cisco 7600 series router using the **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 IOS 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.
	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 **set ip default next-hop** command in route-map configuration mode. To delete an entry, use the **no** form of this command.

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

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

Syntax Description

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

Defaults

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 **set ip default next-hop** command needs to be adjacent to the router. The optional specified IP addresses are tried in turn.

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

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

1. **set ip next-hop**
2. **set interface**

3. set ip default next-hop**4. set default interface****Note**

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

Examples

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

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

Related Commands

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

no set ip default next-hop verify-availability

Syntax Description This command has no arguments or keywords.

Defaults 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 **set ip global** command in route-map configuration mode. To disable this feature, use the **no** form of this command.

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

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

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.
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.

Command	Description
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, use the **no** form of this command.

```
set ip next-hop {ip-address [...ip-address] | recursive ip-address}
```

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

Syntax Description

<i>ip-address</i>	IP address of the next hop to which packets are output. It must be the address of an adjacent router.
recursive <i>ip-address</i>	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.

Defaults

This command is disabled by default.

Command Modes

Route-map configuration

Command History

Release	Modification
11.0	This command was introduced.
12.0(28)S	The recursive keyword was added.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

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 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.

If the interface associated with the first next hop 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 **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

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

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

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

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

Related Commands

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

set ip next-hop verify-availability

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

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

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

Syntax Description

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

Command Default

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

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.3(4)T	The optional track keyword and <i>next-hop-address</i> , <i>sequence</i> , and <i>object</i> arguments were added.
12.3(14)T	The SAA feature (uses rtr commands) was replaced by the IP SLAs feature (uses ip sla 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.

Usage Guidelines

The **set ip next-hop verify-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 **set ip next-hop verify-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 **set ip next-hop verify-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 **set ip next-hop verify-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
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
route-map Example1 permit 20
 match ip address 101
  set interface Ethernet0/0/3
  set ip tos max-throughput
```

Using Object Tracking

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

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

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

Related Commands

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 **set ip vrf** command in route-map configuration mode. To disable this feature, use the **no** form of this command.

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

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

Syntax Description

<i>vrf-name</i>	Name of the VRF.
next-hop <i>ip-address</i>	IP address of the next hop to which packets are forwarded. The next hop must be an adjacent router.
next-hop recursive <i>ip-address</i>	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)SRB1	This command was introduced.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.

Usage Guidelines

The **set ip vrf** 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 **ip policy route-map** interface configuration command, the **route-map** global configuration command, and **match** 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.

If the interface associated with the first next hop specified with the **set ip vrf** 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 Cisco IOS software has no explicit route to a destination.
set ip next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing.

set level (IP)

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

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

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

Syntax Description

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

Defaults

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.
12.2(33)SRE	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 *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** 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.

The **stub-area** and **backbone** keywords have no effect on where routes are imported.

Examples

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

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

Related Commands

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

set local-preference

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

set local-preference *number-value*

no set local-preference *number-value*

Syntax Description

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

Defaults

Preference value of 100

Command Modes

Route-map configuration

Command History

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

Usage Guidelines

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

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

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

You can change the default preference value with the **bgp default local-preference** command.

Examples

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

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

Related Commands

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

set metric (BGP-OSPF-RIP)

To set the metric value for a routing protocol, use the **set metric** 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

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

Defaults

The dynamically learned metric value.

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

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 **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 metric value for the routing protocol to 100:

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

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community	Matches a BGP community.
match interface (IP)	Distributes routes that have their next hop out one of the interfaces specified.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match ip next-hop	Redistributes any routes that have a next hop router address passed by one of the access lists specified.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match metric (IP)	Redistributes routes with the metric specified.
match route-type (IP)	Redistributes routes of the specified type.
match tag	Redistributes routes in the routing table that match the specified tags.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set automatic-tag	Automatically computes the tag value.
set community	Sets the BGP communities attribute.
set ip next-hop	Specifies the address of the next hop.
set level (IP)	Indicates where to import routes.
set local-preference	Specifies a preference value for the autonomous system path.
set metric (BGP, OSPF, RIP)	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
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 **set metric-type** command in route-map configuration mode. To return to the default, use the **no** form of this command.

```
set 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.

Defaults

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 *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** 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.



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

set next-hop *next-hop*

no set next-hop *next-hop*

Syntax Description

next-hop IP address of the next hop router.

Defaults

Default next hop address.

Command Modes

Route-map configuration

Command History

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

Usage Guidelines

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

Use the **route-map** global configuration command, and the **match** and **set** route-map configuration commands, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the *set actions*—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **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 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.
set tag (IP)	Sets the value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.

set tag (IP)

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

set tag *tag-value*

no set tag *tag-value*

Syntax Description

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

Command Default

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

Command Modes

Route-map configuration (config-route-map)

Command History

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

Usage Guidelines

Use the **route-map** global configuration command, and the **match** and **set** route-map configuration commands, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *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** 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 tag value of the destination routing protocol to 5:

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

Related Commands

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

show bfd drops

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

show bfd drops

Syntax Description This command has no arguments or keywords.

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

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

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

```
Router# show bfd drops

BFD Drop Statistics

```

	IPV4	IPV6	MPLS_PW	MPLS_TP_LSP
Invalid TTL	0	0	0	0
BFD Not Configured	0	0	0	0
No BFD Adjacency	0	0	0	0
Invalid Header Bits	0	0	0	0
Invalid Discriminator	0	0	0	0
Session AdminDown	0	0	0	0

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

show bfd neighbors

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

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

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

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

Command History	S Release	Modification
	12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S.
	12.2(18)SXE	This command was introduced.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2(33)SRC	This command was modified. The vrf vrf-name keyword and argument, the client keyword, and the <i>ip-address</i> argument were added.
	12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
	12.2(33)SXI	This command was modified. The output was modified to display the “OurAddr” field only with the details keyword.

12.2(33)SRE	This command was modified. Support for IPv6 was added.
15.1(2)S	This command was modified. <ul style="list-style-type: none"> The show bfd neighbors details command output was changed for hardware-offloaded BFD sessions. The show bfd neighbors command output was changed to show the header type identifying the session type.
T Release	Modification
12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.
12.4(9)T	This command was modified. Support for BFD Version 1 and BFD echo mode was added.
15.1(2)T	This command was modified. Support for IPv6 was added.
X Release	Modification
Cisco IOS XE Release 2.1	This command was modified. Support for IPv6 was added.

Usage Guidelines

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

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

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

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

Examples

Examples for Cisco IOS Release 12.0(31)S, 12.2(18)SXE, 12.2(33)SRA, 12.2(33)SB, and 12.4(4)T

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

```
Router# show bfd neighbors

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

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

```
Router# show bfd neighbors details

NeighAddr                LD/RD  RH/RS  State  Int
10.1.1.2                  1/1    1(RH)  Up     Et0/0
Session state is UP and not using echo function.
OurAddr: 10.1.1.1
Local Diag: 0, Demand mode: 0, Poll bit: 0
```

```

MinTxInt: 50000, MinRxInt: 50000, Multiplier: 3 Received MinRxInt: 50000, Received
Multiplier: 3 Holddown (hits): 150(0), Hello (hits): 50(2223) Rx Count: 2212, Rx Interval
(ms) min/max/avg: 8/68/49 last: 0 ms ago Tx Count: 2222, Tx Interval (ms) min/max/avg:
40/60/49 last: 20 ms ago Elapsed time watermarks: 0 0 (last: 0) Registered protocols: CEF
Stub
Uptime: 00:01:49
Last packet: Version: 0 - Diagnostic: 0
                I Hear You bit: 1 - Demand bit: 0
                Poll bit: 0 - Final bit: 0
                Multiplier: 3 - Length: 24
                My Discr.: 1 - Your Discr.: 1
                Min tx interval: 50000 - Min rx interval: 50000
                Min Echo interval: 50000

```

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

```
Router# show bfd neighbors
```

```
Cleanup timer hits: 0
```

OurAddr	NeighAddr	LD/RD	RH	Holdown(mult)	State	Int
172.16.10.2	172.16.10.1	2/0	0	0 (0)	Up	Fa6/0

Total Adjs Found: 1

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

```
Router# show bfd neighbors details
```

```
Cleanup timer hits: 0
```

OurAddr	NeighAddr	LD/RD	RH	Holdown(mult)	State	Int
172.16.10.2	172.16.10.1	2/0	0	0 (0)	Up	Fa6/0

```
Registered protocols: OSPF
```

```
Uptime: never
```

```
%% BFD Neighbor statistics are not available on RP. Please execute this command on Line Card.
```

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

```
Router# attach 6
```

```
Entering Console for 8 Port Fast Ethernet in Slot: 6
Type "exit" to end this session
```

```
Press RETURN to get started!
```

```
Router> show bfd neighbors
```

```
Cleanup timer hits: 0
```

OurAddr	NeighAddr	LD/RD	RH	Holdown(mult)	State	Int
172.16.10.2	172.16.10.1	2/1	1	848 (5)	Up	Fa6/0

Total Adjs Found: 1

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

```
Router# attach 6
```

```
Entering Console for 8 Port Fast Ethernet in Slot: 6
Type "exit" to end this session
```

show bfd neighbors

Press RETURN to get started!

Router> **show bfd neighbors details**

Cleanup timer hits: 0

```
OurAddr      NeighAddr    LD/RD RH   Holddown(mult)  State   Int
172.16.10.2  172.16.10.1  2/1  1   892 (5 )        Up      Fa6/0
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 1000, Multiplier: 3
Received MinRxInt: 200000, Received Multiplier: 5
Holddown (hits): 1000(0), Hello (hits): 200(193745)
Rx Count: 327406, Rx Interval (ms) min/max/avg: 152/248/196 last: 108 ms ago
Tx Count: 193748, Tx Interval (ms) min/max/avg: 204/440/331 last: 408 ms ago
Last packet: Version: 0          - Diagnostic: 0
                    I Hear You bit: 1      - Demand bit: 0
                    Poll bit: 0           - Final bit: 0
                    Multiplier: 5         - Length: 24
                    My Discr.: 1          - Your Discr.: 2
                    Min tx interval: 200000 - Min rx interval: 200000
                    Min Echo interval: 0
Uptime: 17:54:07
SSO Cleanup Timer called: 0
SSO Cleanup Action Taken: 0
Pseudo pre-emptive process count: 7728507 min/max/avg: 8/16/8 last: 12 ms ago
IPC Tx Failure Count: 0
IPC Rx Failure Count: 0
Total Adjs Found: 1
LC-Slot6>
```

Example for 12.4(9)T and Later Releases

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

Router# **show bfd neighbors details**

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

Example for Cisco IOS XE Release 2.1 and Later Releases

The following example displays all IPv6 sessions:

Router# **show bfd neighbors ipv6 2001::1**

```
OurAddr      NeighAddr    LD/RD RH/RS   Holddown(mult)  State   Int
1::5         1::6         2/2   Up      0 (3 )          Up      Et0/0
```

```
2:2::5      2:2::6      4/4      Up      0      (3 )      Up      Et1/0
```

Examples for Cisco IOS Release 12.2(33)SXI, 12.2(33)SRE, 12.2(33)XNA, and Later Releases

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

```
Router# show bfd neighbors
```

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

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

```
Router# show bfd neighbors details
```

NeighAddr	LD/RD	RH/RS	State	Int
192.0.2.5	4/0	Down	Down	Et0/0

```

OurAddr: 192.0.2.8
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3
Received MinRxInt: 0, Received Multiplier: 0
Holddown (hits): 0(0), Hello (hits): 1000(120)
Rx Count: 0, Rx Interval (ms) min/max/avg: 0/0/0 last: 118672 ms ago
Tx Count: 120, Tx Interval (ms) min/max/avg: 760/1000/885 last: 904 ms ago
Elapsed time watermarks: 0 0 (last: 0)
Registered protocols: Stub
Last packet: Version: 1          - Diagnostic: 0
              State bit: AdminDown - Demand bit: 0
              Poll bit: 0         - Final bit: 0
              Multiplier: 0       - Length: 0
              My Discr.: 0        - Your Discr.: 0
              Min tx interval: 0  - Min rx interval: 0
              Min Echo interval: 0

```

NeighAddr	LD/RD	RH/RS	State	Int
1000:1:1:1:1:1:2	9/0	Down	Down	Et0/0

```

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

```



```
Min Echo interval: 0
```

Table 2 describes the significant fields shown in the displays.

Table 2 *show bfd neighbors Field Descriptions*

Field	Description
OurAddr	IP address of the interface for which the show bfd neighbors details command was entered.
NeighAddr	IPv4 or IPv6 address of the BFD adjacency or neighbor.
LD/RD	Local discriminator and remote discriminator being used for the session.
RH	Remote Heard—Indicates that the remote BFD neighbor has been heard.
Holdown(mult)	The detect timer multiplier that is used for this session.
State	State of the interface—Up or Down.
Int	Interface type and slot/port.
Session state is UP and using echo function with 50 ms interval.	BFD is up and running in echo mode. The 50-millisecond interval has been adopted from the bfd command. Note BFD Version 1 and echo mode are supported only with Cisco IOS Release 12.4(9)T and later releases.
Rx Count	Number of BFD control packets that have been received from the BFD neighbor.
Tx Count	Number of BFD control packets that have been sent by the BFD neighbor.
Tx Interval	The interval, in milliseconds, between sent BFD packets.
Registered protocols	Routing protocols that have been registered with BFD.
Last packet: Version:	BFD version detected and run between the BFD neighbors. The system automatically performs BFD version detection, and BFD sessions between neighbors will run in the highest common BFD version between neighbors. For example, if one BFD neighbor is running BFD Version 0, and the other BFD neighbor is running Version 1, the session will run BFD Version 0. Note BFD Version 1 and echo mode are supported only with Cisco IOS Release 12.4(9)T and later releases.
Diagnostic	A diagnostic code specifying the local system's reason for the last transition of the session from Up to some other state. State values are as follows: <ul style="list-style-type: none"> • 0—No Diagnostic • 1—Control Detection Time Expired • 2—Echo Function Failed • 3—Neighbor Signaled Session Down • 4—Forwarding Plane Reset • 5—Path Down • 6—Concentrated Path Down • 7—Administratively Down

Table 2 *show bfd neighbors Field Descriptions (continued)*

Field	Description
I Hear You bit	The I Hear You Bit is set to 0 if the transmitting system is either not receiving BFD packets from the remote system or is tearing down the BFD session for some reason. During normal operation, the I Hear You bit is set to 1 to signify that the remote system is receiving the BFD packets from the transmitting system.
Demand bit	Demand Mode bit. BFD has two modes—asynchronous and demand. If the Demand Mode is set, the transmitting system prefers to operate in demand mode. The Cisco implementation of BFD supports only asynchronous mode.
Poll bit	If the Poll bit is set, the transmitting system is requesting verification of connectivity or verification of a parameter change.
Final bit	If the Final bit is set, the transmitting system is responding to a received BFD control packet that had a Poll (P) bit set.
Multiplier	Detect time multiplier. The negotiated transmit interval multiplied by the detect time multiplier determines the detection time for the transmitting system in BFD asynchronous mode. The detect time multiplier is similar to the hello multiplier in Intermediate System-to-Intermediate System (IS-IS), which is used to determine the hold timer: (hello interval) * (hello multiplier) = hold timer. If a hello packet is not received within the hold-timer interval, a failure has occurred. Similarly, for BFD: (transmit interval) * (detect multiplier) = detect timer. If a BFD control packet is not received from the remote system within the detect-timer interval, a failure has occurred.
Length	Length of the BFD control packet, in bytes.
My Discr.	My Discriminator. Unique, nonzero discriminator value generated by the transmitting system used to demultiplex multiple BFD sessions between the same pair of systems.
Your Discr.	Your Discriminator. The discriminator received from the corresponding remote system. This field reflects the received value of My Discriminator, or is zero if that value is unknown.
Min tx interval	Minimum transmission interval, in microseconds, that the local system wants to use when sending BFD control packets.
Min rx interval	Minimum receipt interval, in microseconds, between received BFD control packets that the system can support.
Min Echo interval	Minimum interval, in microseconds, between received BFD control packets that the system can support. If the value is zero, the transmitting system does not support the receipt of BFD echo packets. The Cisco implementation of BFD for Cisco IOS Releases 12.2(18)SXE and 12.0(31)S does not support the use of echo packets.

Example for Cisco IOS Release 15.1(2)S with Hardware Offload to Cisco 7600 Series Routers

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

show bfd neighbors

```

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

```

Examples for Cisco IOS Release 15.1(2)S with Changes in the Header Line in the Output

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

```
Router# show bfd neighbors
```

MPLS-TP Sessions

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

IPv4 Sessions

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

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

```
Router# show bfd neighbors
```

VCCV Sessions

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

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

```
Router# show bfd neighbors
```

IPv4 Sessions

NeighAddr	LD/RD	RH/RS	State	Int
192.0.2.1	6/0	Down	Down	Et1/0
203.0.113.1	7/6	Up	Up	Et3/0
198.51.100.2	8/7	Up	Up	Et0/0

IPv6 Sessions

NeighAddr	LD/RD	RH/RS	State	Int
CC::2	1/1	Up	Up	Et0/0

```

DD::2                2/2    Up      Up      Et0/0
EE::2                3/3    Up      Up      Et0/0
ABCD::2              4/4    Up      Up      Et0/0
FE80::2              5/5    Up      Up      Et0/0

```

Table 3 describes the significant fields shown in the displays.

Table 3 *show bfd neighbors Field Descriptions*

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

Related Commands

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

show dampening interface

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

show dampening interface

Syntax Description This command has no arguments or keywords.

Command Modes User EXEC
Privileged EXEC

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

Examples The following is sample output from the **show dampening interface** 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
```

[Table 4](#) describes the significant fields shown in the sample output of the **show dampening interface** command.

Table 4 *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 interface dampening

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

show interface dampening

Syntax Description This command has no keywords or arguments.

Command Modes EXEC

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

Examples The following is sample output from the **show interface dampening** command:

```
Router# show interface dampening
```

```
Flaps Penalty Supp ReuseTm HalfL ReuseV SuppV MaxSTm MaxP Restart
      0      0 FALSE      0      5  1000  2000      20  16000      0
```

[Table 5](#) describes the significant fields shown in the display.

Table 5 *show interface dampening Field Descriptions*

Field	Description
Flaps	Displays the number of times that an interface has flapped.
Penalty	Displays the accumulated penalty.
Supp	Indicates if the interface is dampened.
ReuseTm	Displays the reuse timer.
HalfL	Displays the half-life counter.
ReuseV	Displays the reuse threshold timer.
SuppV	Displays the suppress threshold.
MaxSTm	Displays the maximum suppress.
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 static route bfd

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

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

Syntax Description

group	(Optional) Specifies a BFD group.
<i>group-name</i>	(Optional) BFD group name.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

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

Usage Guidelines

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

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

Examples

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

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

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

[Table 6](#) describes the significant fields shown in the display.

Table 6 show ip static route bfd Field Descriptions

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

Table 6 *show ip static route bfd Field Descriptions (continued)*

Field	Description
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 **show ip cache policy** command in EXEC mode.

show ip cache policy

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

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

Examples

The following is sample output from the **show ip cache policy** command:

```
Router# show ip cache policy
```

```
Total adds 10, total deletes 10
```

```
Type  Routemap/sequence      Age      Interface      Next Hop
NH   george/10                00:04:31 Ethernet0      192.168.1.2
Int  george/30                00:01:23 Serial4        192.168.5.129
```

[Table 7](#) describes the significant fields shown in the display.

Table 7 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 set ip next-hop command. “Int” indicates the set interface command.
Routemap	Name of the route map that created the entry; in this example, george.
sequence	Route map sequence number.
Age	Age of the cache entry.
Interface	Output interface type and number.
Next Hop	IP address of the next hop.

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 **show ip local policy** command in EXEC mode.

show ip local policy

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

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

Examples The following is sample output from the **show ip local policy** command:

```
Router# show ip local policy

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

Table 8 describes the significant fields shown in the display.

Table 8 *show ip local policy Field Descriptions*

Field	Description
route-map equal	The name of the route map is equal.
permit	The route map contains permit statements.
sequence	The sequence number of the route map, which determines in what order it is processed among other route maps.
Match clauses:	Clauses in the route map that must be matched to satisfy the permit or deny action.

Table 8 *show ip local policy Field Descriptions (continued)*

Field	Description
Set clauses:	Set clauses that will be put into place if the match clauses are met.
Policy routing matches: packets	Number of packets that meet the match clauses.
bytes	Number of bytes in the packets that meet the match clauses.

Related Commands

Command	Description
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 **show ip policy** 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 **show ip policy** 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 **show route-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
```

Table 9 describes the significant fields shown in the display.

Table 9 *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.
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 **show ip protocols** command in privileged EXEC mode.

show ip protocols

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC (#)

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

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

Once you configure the **default-information originate on-passive** command, the output of the **show ip protocols** command displays that RIP default routes are sent on passive interfaces.

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

```
Router# show ip protocols

*** IP Routing is NSF aware ***

Routing Protocol is "eigrp 3"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Default networks flagged in outgoing updates
Default networks accepted from incoming updates
Redistributing: eigrp 3
EIGRP-IPv4 VR(test) Address-Family Protocol for AS(3)
Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
NSF-aware route hold timer is 240
```

```

Router-ID: 10.1.1.1
Topology : 0 (base)
Active Timer: 3 min
Distance: internal 90 external 170
Maximum path: 4
Maximum hopcount 100
Maximum metric variance 1
Total Prefix Count: 3
Total Redist Count: 0

Automatic Summarization: disabled
Maximum path: 4
Routing for Networks:
10.0.0.0
Routing Information Sources:
Gateway Distance Last Update
10.1.1.2 90 00:05:10
Distance: internal 90 external 170

```

Table 10 describes the significant fields shown in the display.

Table 10 *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-list out command.
Incoming update filter list for all interfaces...	Indicates whether a filter for incoming routing updates has been specified with the distribute-list in 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).
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.

Table 10 *show ip protocols Field Descriptions (continued)*

Field	Description
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: <ul style="list-style-type: none"> • IP address • Administrative distance • Time the last update was received from this source

IS-IS Example

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

```
Router# show ip protocols

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

[Table 11](#) describes the significant fields shown in the display.

Table 11 *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.

Table 11 *show ip protocols Field Descriptions for an IS-IS Process (continued)*

Field	Description
Routing	Specifies the networks for which the routing process is currently injecting routes.
Routing Information Sources	Lists all the routing sources the Cisco IOS software is using to build its routing table. For each source, you will see the following displayed: <ul style="list-style-type: none"> • IP address • Administrative distance • Time the last update was received from this source

RIP Example

The following sample output from the **show ip protocols** command displays RIP processes:

```
Router# show ip protocols

Routing Protocol is "rip"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Sending updates every 30 seconds, next due in 6 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Sending Default route on Passive interfaces
  Redistributing: rip
  Default version control: send version 2, receive version 2
  Automatic network summarization is not in effect
  Maximum path: 4
  Routing for Networks:
    172.19.0.0
    10.2.0.0
    10.3.0.0
  Passive Interface(s):
    Ethernet0/0
    Ethernet0/1
    Ethernet0/2
    Ethernet0/3
    Ethernet1/0
    Ethernet1/1
    Ethernet1/2
    Ethernet1/3
  Passive Interface(s):
    Serial2/0
    Serial2/1
    Serial2/2
    Serial2/3
    Serial3/0
    Serial3/1
    Serial3/2
    Serial3/3
  Routing Information Sources:
    Gateway          Distance      Last Update
  Distance: (default is 120)
```

Table 12 describes the significant fields shown in the display.

Table 12 *show ip protocols Field Descriptions for a RIP Process*

Field	Description
Routing Protocol is "rip"	Specifies the routing protocol used.
Outgoing update ...	Specifies whether the outgoing filtering list has been set.
Incoming update ...	Specifies whether the incoming filtering list has been set.
Sending updates every 30 seconds	Specifies the time (in seconds) between sending updates.
next due in 6 seconds	Specifies when the next update is due to be sent.
Invalid after 180 seconds	Specifies the value of the invalid parameter.
hold down 180	Specifies the current value of the hold-down parameter.
flushed after 240	Specifies the time (in seconds) after which the individual routing information will be thrown (flushed) out.
Sending Default route on Passive interfaces	Specifies that RIP update packets are sent only with a default route on passive interfaces.
Redistributing	Lists the protocol that is being redistributed.
Default version control:	Specifies the version of RIP packets that are sent and received.
Routing	Specifies the networks for which the routing process is currently injecting routes.
Routing Information Sources	Lists all the routing sources the Cisco IOS software is using to build its routing table. For each source, you will see the following displayed: <ul style="list-style-type: none"> • IP address • Administrative distance • Time the last update was received from this source

EIGRP NSF Awareness Verification Example

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

```
Router# show ip protocols

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

```
Distance: internal 90 external 170
```

Table 13 describes the significant fields shown in the display.

Table 13 *show ip protocols Field Descriptions for an EIGRP NSF-Aware Process*

Field	Description
Routing Protocol is "eigrp 101"	Specifies the routing protocol used.
Outgoing update ...	Specifies whether the outgoing filtering list has been set.
Incoming update ...	Specifies whether the incoming filtering list has been set.
Default networks...	Specifies how these networks will be handled in both incoming and outgoing updates.
EIGRP...	Specifies the value of the K0–K5 metrics, and the maximum hop count.
Redistributing	Lists the protocol that is being redistributed.
EIGRP NSF-Aware...	Displays the route-hold timer value.
Automatic network summarization...	Specifies that automatic summarization is enabled.
Routing	Specifies the networks for which the routing process is currently injecting routes.
Routing Information Sources	Lists all the routing sources the Cisco IOS software is using to build its routing table. For each source, you will see the following displayed: <ul style="list-style-type: none"> • IP address • Administrative distance • Time the last update was received from this source

Related Commands

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

show ip route

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

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

Syntax Description

<i>ip-address</i>	(Optional) IP address about which routing information should be displayed.
repair-paths	(Optional) Displays the repair paths.
next-hop-override	(Optional) Displays the next hop overrides (NHRP) associated with a particular route, along with the corresponding default next hops.
dhcp	(Optional) Displays routes added by the Dynamic Host Configuration Protocol (DHCP) server.
<i>mask</i>	(Optional) The subnet mask.
longer-prefixes	(Optional) Specifies that only routes matching the <i>ip-address</i> and <i>mask</i> pair should be displayed.
<i>protocol</i>	(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 , nhp , and rip .
<i>process-id</i>	(Optional) The number used to identify a process of the specified protocol.
list	(Optional) Filters output by an access list name or number.
<i>access-list-number</i>	(Optional) Specific access list number for which output from the routing table should be displayed.
<i>access-list-name</i>	(Optional) Specific access list name for which output from the routing table should be displayed.
static	(Optional) Displays static routes.
download	(Optional) Displays route installed using the Authentication, Authorization, and Accounting (AAA) route download function. This keyword is used only when AAA is configured.
update-queue	(Optional) Displays Routing Information Base (RIB) queue updates.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
9.2	This command was introduced.
10.0	The “D—EIGRP, EX—EIGRP, N1—OSPF NSSA external type 1 route” and “N2—OSPF NSSA external type 2 route” codes were added to the command output.

Release	Modification
10.3	The <i>process-id</i> argument was added.
11.0	The longer-prefixes keyword was added.
11.1	The “U—per-user static route” code was added to the command output.
11.2	The “o—on-demand routing” code was added to the command output.
12.2(33)SRA	This command was modified. The update-queue keyword was added.
11.3	The output from the show ip route <i>ip-address</i> command was enhanced to display the origination of an IP route in Intermediate System-to-Intermediate System (IS-IS) networks.
12.0(1)T	The “M—mobile” code was added to the command output.
12.0(3)T	The “P—periodic downloaded static route” code was added to the command output.
12.0(4)T	The “ia—IS-IS” code was added to the command output.
12.2(2)T	The output from the show ip route <i>ip-address</i> command was enhanced to display information on the multipaths to the specified network.
12.2(13)T	The <i>egp</i> and <i>igrp</i> arguments were removed because the exterior gateway protocol (EGP) and the Interior Gateway Routing Protocol (IGRP) are no longer available in Cisco IOS 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	The output was enhanced to display route tag information.
12.3(8)T	The output was enhanced to display static routes using DHCP.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRE	This command was modified. The dhcp and repair-paths keywords were added. Support for the Border Gateway Protocol (BGP) best external and BGP additional path features was added.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was modified. The next-hop-override and nhrp keywords were added.

Usage Guidelines

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

Examples

Routing Table Examples

The following examples show the standard routing tables displayed by the **show ip route** command. Use the codes displayed at the beginning of each report and the information in [Table 14](#) to understand the type of route.

The following is sample output from the **show ip route** command when entered without an address:

```
Router# show ip route
```

```
Codes: R - RIP derived, O - OSPF derived,
```


show ip route

```

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

```

Gateway of last resort is 10.119.254.240 to network 10.140.0.0

```

O E2 10.110.0.0 [160/5] via 10.119.254.6, 0:01:00, Ethernet2
E   10.67.10.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
O E2 10.68.132.0 [160/5] via 10.119.254.6, 0:00:59, Ethernet2
O E2 10.130.0.0 [160/5] via 10.119.254.6, 0:00:59, Ethernet2
E   10.128.0.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E   10.129.0.0 [200/129] via 10.119.254.240, 0:02:22, Ethernet2
E   10.65.129.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E   10.10.0.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E   10.75.139.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
E   10.16.208.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E   10.84.148.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
E   10.31.223.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E   10.44.236.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
E   10.141.0.0 [200/129] via 10.119.254.240, 0:02:22, Ethernet2
E   10.140.0.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2

```

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

```
Router# show ip route
```

```

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

```

Gateway of last resort is not set

```

10.89.0.0 is subnetted (mask is 255.255.255.0), 3 subnets
C   10.89.64.0 255.255.255.0 is possibly down,
    routing via 0.0.0.0, Ethernet0
i L2 10.89.67.0 [115/20] via 10.89.64.240, 0:00:12, Ethernet0
i L2 10.89.66.0 [115/20] via 10.89.64.240, 0:00:12, Ethernet0

```

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

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

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

```

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

```

E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
N2 - OSPF NSSA external type 2 route

Gateway of last resort is not set

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

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

Router# **show ip route**

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

Gateway of last resort is 172.21.17.1 to network 0.0.0.0

```
172.31.0.0/32 is subnetted, 1 subnets
P 172.31.229.41 is directly connected, Dialer1 20.0.0.0/24 is subnetted, 3 subnets
P 10.1.1.0 [200/0] via 172.31.229.41, Dialer1
P 10.1.3.0 [200/0] via 172.31.229.41, Dialer1
P 10.1.2.0 [200/0] via 172.31.229.41, Dialer1
```

Router# **show ip route static**

```
172.27.4.0/8 is variably subnetted, 2 subnets, 2 masks
P 172.16.1.1/32 is directly connected, BRI0
P 172.27.4.0/8 [1/0] via 10.1.1.1, BRI0
S 172.31.0.0/16 [1/0] via 172.21.114.65, Ethernet0
S 10.0.0.0/8 is directly connected, BRI0
P 10.0.0.0/8 is directly connected, BRI0
172.21.0.0/16 is variably subnetted, 5 subnets, 2 masks
S 172.21.114.201/32 is directly connected, BRI0
S 172.21.114.205/32 is directly connected, BRI0
S 172.21.114.174/32 is directly connected, BRI0
S 172.21.114.12/32 is directly connected, BRI0
P 10.0.0.0/8 is directly connected, BRI0
P 10.1.0.0/16 is directly connected, BRI0
P 10.2.2.0/24 is directly connected, BRI0
```

```
S* 0.0.0.0/0 [1/0] via 172.21.114.65, Ethernet0
S 172.29.0.0/16 [1/0] via 172.21.114.65, Ethernet0
```

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

```
Router# show ip route static download

Connectivity: A - Active, I - Inactive

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

The following example shows how to use the **show ip route nhrp** command to enable shortcut switching on the tunnel interface:

```
Router# show ip route

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

Gateway of last resort is not set

10.0.0.0/16 is variably subnetted, 3 subnets, 2 masks
C 10.1.1.0/24 is directly connected, Tunnel0
C 172.16.22.0 is directly connected, Ethernet1/0
H 172.16.99.0 [250/1] via 10.1.1.99, 00:11:43, Tunnel0
10.11.0.0/24 is subnetted, 1 subnets
C 10.11.11.0 is directly connected, Ethernet0/0
```

```
Router# show ip route nhrp

H 172.16.99.0 [250/1] via 10.1.1.99, 00:11:43, Tunnel0
```

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

```
=====
1) Initial configuration
=====
Router# show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
```

```
o - ODR, P - periodic downloaded static route, H - NHRP
+ - replicated route
```

Gateway of last resort is not set

```
10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C    10.2.1.0/24 is directly connected, Loopback1
L    10.2.1.1/32 is directly connected, Loopback1
10.0.0.0/24 is subnetted, 1 subnets
S    10.10.10.0 is directly connected, Tunnel0
10.11.0.0/24 is subnetted, 1 subnets
S    10.11.11.0 is directly connected, Ethernet0/0
```

Router# **show ip route next-hop-override**

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

Gateway of last resort is not set

```
10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C    10.2.1.0/24 is directly connected, Loopback1
L    10.2.1.1/32 is directly connected, Loopback1
10.0.0.0/24 is subnetted, 1 subnets
S    10.10.10.0 is directly connected, Tunnel0
10.11.0.0/24 is subnetted, 1 subnets
S    10.11.11.0 is directly connected, Ethernet0/0
```

Router# **show ip cef**

Prefix	Next Hop	Interface
.	.	.
10.2.1.255/32	receive	Loopback1
10.10.10.0/24	attached	Tunnel0 <<<<<<<<
10.11.11.0/24	attached	Ethernet0/0
127.0.0.0/8	drop	

2) Add a Nexthop-override

```
address = 10.10.10.0
mask = 255.255.255.0
gateway = 10.1.1.1
interface = Tunnel0
```

Router# **show ip route**

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

show ip route

```

Gateway of last resort is not set

    10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       10.2.1.0/24 is directly connected, Loopback1
L       10.2.1.1/32 is directly connected, Loopback1
    10.0.0.0/24 is subnetted, 1 subnets
% S      10.10.10.0 is directly connected, Tunnel0
    10.11.0.0/24 is subnetted, 1 subnets
S       10.11.11.0 is directly connected, Ethernet0/0

```

Router# **show ip route next-hop-override**

```

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

```

```

Gateway of last resort is not set

    10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       10.2.1.0/24 is directly connected, Loopback1
L       10.2.1.1/32 is directly connected, Loopback1
    10.0.0.0/24 is subnetted, 1 subnets
% S      10.10.10.0 is directly connected, Tunnel0
           [NHO] [1/0] via 10.1.1.1, Tunnel0
    10.11.0.0/24 is subnetted, 1 subnets
S       10.11.11.0 is directly connected, Ethernet0/0

```

Router# **show ip cef**

Prefix	Next Hop	Interface
.		
.		
.		
10.2.1.255/32	receive	Loopback110.10.10.0/24
10.10.10.0/24	10.1.1.1	Tunnel0
10.11.11.0/24	attached	Ethernet0/0
10.12.0.0/16	drop	
.		
.		
.		

```

=====
3) Delete a Nexthop-override
   address = 10.10.10.0
   mask = 255.255.255.0
   gateway = 10.11.1.1
   interface = Tunnel0
=====

```

Router# **show ip route**

```

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

```

+ - replicated route

Gateway of last resort is not set

```

10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C    10.2.1.0/24 is directly connected, Loopback1
L    10.2.1.1/32 is directly connected, Loopback1
10.0.0.0/24 is subnetted, 1 subnets
S    10.10.10.0 is directly connected, Tunnel0
10.11.0.0/24 is subnetted, 1 subnets
S    10.11.11.0 is directly connected, Ethernet0/0

```

Router# **show ip route next-hop-override**

```

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

```

Gateway of last resort is not set

```

10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C    10.2.1.0/24 is directly connected, Loopback1
L    10.2.1.1/32 is directly connected, Loopback1
10.0.0.0/24 is subnetted, 1 subnets
S    10.10.10.0 is directly connected, Tunnel0
10.11.0.0/24 is subnetted, 1 subnets
S    10.11.11.0 is directly connected, Ethernet0/0

```

Router# **show ip cef**

Prefix	Next Hop	Interface
.		
.		
.		
10.2.1.255/32	receive	Loopback10.10.10.0/24
10.10.10.0/24	attached	Tunnel0
10.11.11.0/24	attached	Ethernet0/0
10.120.0.0/16	drop	
.		
.		
.		

Table 14 show ip route Field Descriptions

Field	Description
Codes	<p>Indicates the protocol that derived the route. It can be one of the following values:</p> <ul style="list-style-type: none"> • B—BGP derived • C—connected • D—Enhanced Interior Gateway Routing Protocol (EIGRP) • EX—EIGRP external • H—NHRP • i—IS-IS derived • ia—IS-IS • L—local • M—mobile • O—Open Shortest Path First (OSPF) derived • P—periodic downloaded static route • R—Routing Information Protocol (RIP) derived • S—static • U—per-user static route • o—on-demand routing • +—replicated route
Codes	<p>Type of route. It can be one of the following values:</p> <p>*—Indicates the last path used when a packet was forwarded. It pertains only to the nonfast-switched packets. However, it does not indicate which path will be used next when forwarding a nonfast-switched packet, except when the paths are equal cost.</p> <ul style="list-style-type: none"> • E1—OSPF external type 1 route • E2—OSPF external type 2 route • IA—OSPF inter area route • L1—IS-IS Level 1 route • L2—IS-IS Level 2 route • N1—OSPF not-so-stubby area (NSSA) external type 1 route • N2—OSPF NSSA external type 2 route
10.110.0.0	Indicates the address of the remote network.
[160/5]	The first number in the brackets is the administrative distance of the information source; the second number is the metric for the route.
via 10.119.254.6	Specifies the address of the next router to the remote network.
0:01:00	Specifies the last time the route was updated (in hours:minutes:seconds).
Ethernet2	Specifies the interface through which the specified network can be reached.

Specific Route Information

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

```
Router# show ip route 10.0.0.1

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

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

The preceding example shows the output from the **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 where a particular IP route has originated in your network. In the example the route to 10.0.0.1/32 was originated by a router with IP address 10.191.255.247.

[Table 15](#) describes the significant fields shown when using the **show ip route** command with an IP address.

Table 15 *show ip route with IP Address Field Descriptions*

Field	Description
Routing entry for 10.0.0.1/32	Network number and mask.
Known via...	Indicates how the route was derived.
Tag	Integer that is used to implement the route.
type	Indicates the IS-IS route type (Level 1 or Level 2).
Redistributing via...	Indicates the redistribution protocol.
Last update from 10.191.255.251	Indicates the IP address of a router that is the next hop to the remote network and the router interface on which the last update arrived.
Routing Descriptor Blocks:	Displays the next hop IP address followed by the information source.
Route metric	This value is the best metric for this routing descriptor block.
traffic share count	Number of uses for this routing descriptor block.

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

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

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

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

```
Gateway of last resort is not set
```

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

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

```
Router# show ip route 10.22.0.0
```

```
Routing entry for 10.22.0.0/16
  Known via "isis", distance 115, metric 12
  Tag 120, type level-1
  Redistributing via isis
  Last update from 172.19.170.12 on Ethernet2, 01:29:13 ago
  Routing Descriptor Blocks:
    * 172.19.170.12, from 10.3.3.3, via Ethernet2
      Route metric is 12, traffic share count is 1
      Route tag 120
```

Static Routes Using a DHCP Gateway Examples

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

```
Router# show ip route
```

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
```

```

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route

```

Gateway of last resort is 10.0.19.14 to network 0.0.0.0

```

10.0.0.0/24 is subnetted, 1 subnets
C 10.8.8.0 is directly connected, Ethernet1
  10.0.0.0/32 is subnetted, 1 subnets
S 10.1.1.1 [1/0] via 10.8.8.1
  10.0.0.0/32 is subnetted, 1 subnets
S 10.3.2.1 [24/0] via 10.8.8.1
  172.16.0.0/32 is subnetted, 1 subnets
S 172.2.2.2 [1/0] via 10.8.8.1
  10.0.0.0/28 is subnetted, 1 subnets
C 10.0.19.0 is directly connected, Ethernet0
  10.0.0.0/24 is subnetted, 1 subnets
C 10.15.15.0 is directly connected, Loopback0

S* 10.0.0.0/0 [1/0] via 10.0.19.14

```

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

Router# **show ip route repair-paths**

```

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

```

Gateway of last resort is not set

```

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

```

Router# **show ip route repair-paths 10.9.9.9**

```

>Routing entry for 10.9.9.9/32
> Known via "bgp 100", distance 20, metric 0
> Tag 10, type external

```

show ip route

```

> Last update from 192.168.1.2 00:44:52 ago
> Routing Descriptor Blocks:
> * 192.168.1.2, from 192.168.1.2, 00:44:52 ago, recursive-via-conn
>   Route metric is 0, traffic share count is 1
>   AS Hops 2
>   Route tag 10
>   MPLS label: none
> [RPR]192.168.3.2, from 172.16.1.2, 00:44:52 ago
>   Route metric is 0, traffic share count is 1
>   AS Hops 2
>   Route tag 10
>   MPLS label: none

```

Related Commands

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

show ip route loops

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

show ip route loops

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

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

Usage Guidelines

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

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

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



Note

The above configuration is not useful. The same forwarding behavior can be achieved if you configure **ip route 0.0.0.0 0.0.0.0 192.168.1.2**.

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

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

You can use the **show ip route loops** command to view information about this loop.

Examples

The following is sample output from the **show ip route loops** command. The fields are self-explanatory.

```
Router# show ip route loops

default:ipv4:base 192.168.0.0/16 -> base 192.168.1.2 static 00:56:46
default:ipv4:base 0.0.0.0/0 -> base 192.168.5.6 static 00:56:46 N
```

Related Commands

Command	Description
ip route	Establishes static routes.

show ip route profile

To display routing table change statistics, use the **show ip route profile** command in EXEC mode.

show ip route profile

Syntax Description This command has no arguments or keywords.

Defaults 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 **ip route profile** 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/ interval	Fwd-path change	Prefix add	Nexthop Change	Pathcount Change	Prefix 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

Table 16 describes the significant fields shown in the display.

Table 16 *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 **show ip route summary** command in privileged EXEC mode.

show ip route summary

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

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

Examples The following is sample output from the **show ip route summary** command:

```
Router# show ip route summary

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

[Table 17](#) describes the significant fields shown in the display.

Table 17 show ip route summary Field Descriptions

Field	Description
IP routing table name is...	Displays routing table type and table ID.
IP routing table maximum-paths is...	Number of parallel routes supported by this routing table.
Route Source	Routing protocol name, or the connected , static , or internal keyword. “Internal” indicates those routes that are in the routing table that are not owned by any routing protocol.

Table 17 *show ip route summary Field Descriptions (continued)*

Field	Description
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 **show ip route supernets-only** command in privileged EXEC mode.

show ip route supernets-only

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

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

Examples The following is sample output from the **show ip route supernets-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
```

[Table 18](#) describes the significant fields shown in the display.

Table 18 *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).

Table 18 *show ip route supernets-only Field Descriptions*

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 track-table

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

show ip route track-table

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

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]
```

[Table 19](#) describes the significant fields shown in the display.

Table 19 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.

show ip static route

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

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

Syntax Description		
bfd	(Optional)	Displays IPv4 static Bidirectional Forwarding Detection (BFD) neighbor information.
vrf <i>vrf-name</i>	(Optional)	Name of the VRF by which static routing information should be displayed.
topology <i>topology-name</i>	(Optional)	Static route information for the specified topology.
<i>ip-address</i>	(Optional)	Address by which static routing information should be displayed.
<i>mask</i>	(Optional)	Subnet mask.
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 **show ip static route** command:

```
Router# show ip static route

Codes: M - Manual static, A - AAA download, N - IP NAT, D - DHCP,
       G - GPRS, V - Crypto VPN, C - CASA, P - Channel interface processor,
       B - BootP, S - Service selection gateway
       DN - Default Network, T - Tracking object
       L - TL1, E - OER
Codes in []: A - active, N - non-active, B - BFD-tracked, P - permanent
```

[Table 20](#) 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 key chain

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

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

Syntax Description	<i>name-of-chain</i>	(Optional) Name of the key chain to display, as named in the key chain command.
---------------------------	----------------------	--

Defaults 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 **show key chain** command:

```
Router# show key chain

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

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

show monitor event-trace

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

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

Syntax Description		
all-traces	(Optional)	Displays all event trace messages in memory to the console.
<i>component</i>	(Optional)	Name of the Cisco IOS software subsystem component that is the object of the event trace. To get a list of components that support event tracing in this release, use the monitor event-trace ? command.
all		Displays all event trace messages currently in memory for the specified component.
back <i>hour:minute</i>		Specifies how far back from the current time you want to view messages. For example, you can gather messages from the last 30 minutes. The time argument is specified in hours and minutes format (hh:mm).
clock <i>hour:minute</i>		Displays event trace messages starting from a specific clock time in hours and minutes format (hh:mm).
from-boot <i>seconds</i>		Displays event trace messages starting from a specified number of seconds after booting (uptime). To display the uptime, in seconds, enter the show monitor event-trace component from-boot ? command.
latest		Displays only the event trace messages since the last show monitor event-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 show monitor event-trace cef command replaced the show cef events and show ip cef events 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 <i>component</i> 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.

Release	Modification
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 bfd keyword was added as an entry for the <i>component</i> argument to display trace messages relating to crypto fault detection.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

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

Examples

IPC Component Example

The following is sample output from the **show monitor event-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
```

BFD Component for Cisco IOS Release 12.2(18)SXE, 12.0(31)S, and 12.4(4)T

Use the **show monitor event-trace bfd all** 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 **show monitor event-trace all-traces** command. In this example, separate output is provided for each event, and message numbers are interleaved between the events.

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

```

Test1 event trace:
3667: 6840.016:Message type:3 Data=0123456789
3669: 6841.016:Message type:4 Data=0123456789
3671: 6842.016:Message type:5 Data=0123456789
3673: 6843.016:Message type:6 Data=0123456789

Test2 event trace:
3668: 6840.016:Message type:3 Data=0123456789
3670: 6841.016:Message type:4 Data=0123456789
3672: 6842.016:Message type:5 Data=0123456789
3674: 6843.016:Message type:6 Data=0123456789

```

SPA Component Example

The following is sample output from the **show monitor event-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

```

Cisco Express Forwarding Component Examples

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

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

```
Router# show monitor event-trace cef ipv6 all
```

```
00:00:24.612: [Default] *:*/*'00 New FIB table [OK]
```

```
Router# show monitor event-trace cef ipv4 all
```

```
00:00:24.244: [Default] 127.0.0.81/32'01 FIB insert [OK]
```


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

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

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

The following example shows Cisco Express Forwarding interface events:

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

00:00:24.624: <empty> (sw 4) Create new
00:00:24.624: <empty> (sw 4) SWIDBLnk FastEthernet0/0(4)
00:00:24.624: Fa0/0 (sw 4) NameSet
00:00:24.624: <empty> (hw 1) Create new
00:00:24.624: <empty> (hw 1) HWIDBLnk FastEthernet0/0(1)
00:00:24.624: Fa0/0 (hw 1) NameSet
00:00:24.624: <empty> (sw 3) Create new
00:00:24.624: <empty> (sw 3) SWIDBLnk FastEthernet0/1(3)
00:00:24.624: Fa0/1 (sw 3) NameSet
00:00:24.624: <empty> (hw 2) Create new
```

Cisco Express Forwarding Component Examples for Cisco 10000 Series Routers Only

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

```
Router# show monitor event-trace cef ipv4 all

00:00:48.244: [Default] 127.0.0.81/32'01 FIB insert [OK]
```

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

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

00:00:18.884: SubSys fib_ios_chain init
00:00:18.884: Inst unknown -> RP
00:00:24.584: SubSys fib init
00:00:24.592: SubSys fib_ios init
00:00:24.592: SubSys fib_ios_if init
00:00:24.596: SubSys ipv4fib init
00:00:24.608: SubSys ipv4fib_ios init
00:00:24.620: Flag IPv4 CEF enabled set to yes
```

```

00:00:24.620: Flag      0x7BF6B62C set to yes
00:00:24.620: Flag      IPv4 CEF switching enabled set to yes
00:00:24.624: GState   CEF enabled
00:00:24.628: SubSys   ipv4fib_les init
00:00:24.628: SubSys   ipv4fib_pas init
00:00:24.632: SubSys   ipv4fib_util init
00:00:25.304: Process  Background created
00:00:25.304: Flag      IPv4 CEF running set to yes
00:00:25.304: Process  Background event loop enter
00:00:25.308: Flag      IPv4 CEF switching running set to yes

```

The following examples show Cisco Express Forwarding interface events:

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

```

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

```

CFD Component for Cisco IOS Release 12.4(9)T

To troubleshoot errors in an encryption datapath, enter the **show monitor event-trace cfd all** command. In this example, events are shown separately, each beginning with a time stamp, followed by data from the error trace buffer. Cisco Technical Assistance Center (TAC) engineers can use this information to diagnose the cause of the errors.



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
6BB748F 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 route-map

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

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

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

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	10.0	This command was introduced.
	12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S, and support for continue clauses was integrated into the command output.
	12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
	12.2(27)SBA	The output was enhanced to display dynamically assigned route maps to VRF tables.
	12.2(15)T	An additional counter collect policy routing statistic was integrated into Cisco IOS Release 12.2(15)T.
	12.3(2)T	Support for continue clauses was integrated into Cisco IOS Release 12.3(2)T.
	12.2(17b)SXA	This command was integrated into Cisco IOS Release 12.2(17b)SXA.
	12.3(7)T	The dynamic , application , and all keywords were added.
	12.0(28)S	The support for recursive next-hop clause was added.
	12.3(14)T	The support for recursive next-hop clause was integrated into Cisco IOS Release 12.3(14)T. Support for the map display extension functionality was added. The detailed keyword was added.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
	Cisco IOS XE Release 2.2	In Cisco IOS XE Release 2.2 this command was introduced on the Cisco ASR 1000 Series Routers.
	15.0(1)M	This command was modified. The detailed keyword was removed.

Usage Guidelines

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

Redistribution

Use the **route-map** global configuration command, and the **match** and **set** route-map configuration commands, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the match criteria—the conditions under which redistribution is allowed for the current route-map command. The **set** commands specify the set actions—the particular redistribution actions to perform if the criteria enforced by the match commands are met. The **no route-map** command deletes the route map.

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

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

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

Examples

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

- [show route-map Command with No Keywords Specified: Example, page 188](#)
- [show route-map Command with Dynamic Route Map Specified: Example, page 190](#)
- [show route-map Command with Detailed ACL Information for Route Maps Specified: Example, page 191](#)
- [show route-map Command with VRF Autoclassification: Example, page 191](#)

show route-map Command with No Keywords Specified: Example

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

```
Router# show route-map

route-map ROUTE-MAP-NAME, permit, sequence 10
  Match clauses:
    ip address (access-lists): 1
    metric 10
  Continue: sequence 40
  Set clauses:
    as-path prepend 10
  Policy routing matches: 0 packets, 0 bytes
route-map ROUTE-MAP-NAME, permit, sequence 20
```

```

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

```

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

```

Router# show route-map

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

route-map IN, permit, sequence 10
Match clauses:
  ip address (access-lists): 2
  mpls label
Set clauses:
Policy routing matches: 0 packets, 0 bytes

```

Table 21 describes the significant fields shown in the display.

Table 21 show route-map Field Descriptions

Field	Description
route-map ROUTE-MAP-NAME	Name of the route map.
permit	Indicates that the route is redistributed as controlled by the set actions.
sequence	Number that indicates the position a new route map is to have in the list of route maps already configured with the same name.
Match clauses: tag	Match criteria—Conditions under which redistribution is allowed for the current route map.
Continue:	Continue clause—Shows the configuration of a continue clause and the route-map entry sequence number that the continue clause will go to.

Table 21 *show route-map Field Descriptions (continued)*

Field	Description
Set clauses: metric	Set actions—The particular redistribution actions to perform if the criteria enforced by the match commands are met.
Policy routing matches:	Number of packets and bytes that have been filtered by policy routing.

show route-map Command with Dynamic Route Map Specified: Example

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

```
Router# show route-map dynamic

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

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

```
Router# show route-map dynamic application

Application - AAA
  Number of active routemaps = 1
```

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

```
Router# show route-map dynamic application AAA

AAA
  Number of active rmaps = 2
AAA-02/06/04-14:01:26.619-1-AppSpec
AAA-02/06/04-14:34:09.735-2-AppSpec

Router# show route-map dynamic AAA-02/06/04-14:34:09.735-2-AppSpec

route-map AAA-02/06/04-14:34:09.735-2-AppSpec, permit, sequence 0, identifier 1128046100
  Match clauses:
    ip address (access-lists): PBR#7 PBR#8
  Set clauses:
    Policy routing matches: 0 packets, 0 bytes
```

```

route-map AAA-02/06/04-14:34:09.735-2-AppSpec, permit, sequence 1, identifier 1141277624
  Match clauses:
    ip address (access-lists): PBR#9 PBR#10
  Set clauses:
    Policy routing matches: 0 packets, 0 bytes
route-map AAA-02/06/04-14:34:09.735-2-AppSpec, permit, sequence 2, identifier 1141279420
  Match clauses:
    ip address (access-lists): PBR#11 PBR#12
    length 10 100
  Set clauses:
    ip next-hop 172.16.1.12
    ip gateway 172.16.1.12
    Policy routing matches: 0 packets, 0 bytes
Current active dynamic routemaps = 2

```

show route-map Command with Detailed ACL Information for Route Maps Specified: Example

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

```
Router# show route-map dynamic detailed
```

```

route-map AAA-01/20/04-22:03:10.799-1-AppSpec, permit, sequence 1, identifier 29675368
Match clauses:
ip address (access-lists):
Extended IP access list PBR#3
1 permit icmp 0.0.16.12 1.204.167.240 10.1.1.0 0.0.0.255 syn dscp af12 log-input fragments
Extended IP access list PBR#4
1 permit icmp 0.0.16.12 1.204.167.240 10.1.1.0 0.0.0.255 syn dscp af12 log-input fragments
Set clauses:
ip next-hop 172.16.1.14
ip gateway 172.16.1.14
Policy routing matches: 0 packets, 0 bytes

```

show route-map Command with VRF Autoclassification: Example

The following is sample output from the **show route-map** command when a specified VRF is configured for VRF autoclassification:

```
Router# show route-map dynamic
```

```

route-map None-06/01/04-21:14:21.407-1-IP VRF, permit, sequence 0
identifier 1675771000
Match clauses:
Set clauses: vrf red
Policy routing matches: 0 packets, 0 bytes
Current active dynamic routemaps = 1

```

Related Commands

Command	Description
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
match interface (IP)	Distributes any routes that have their next hop out one of the interfaces specified.
match ip next-hop	Redistributes any routes that have a next hop router address passed by one of the access lists specified.
match tag	Redistributes routes in the routing table that match the specified tags.

traffic-share min

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

traffic-share min across-interfaces

no traffic-share min across-interfaces

Syntax Description

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

Defaults

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

Release 12.2(33)SRB

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

Examples

In the following example, multi-interface load splitting is configured on different interfaces with equal-cost paths:

```
router ospf 5
 traffic-share min across-interfaces
```

VCCV

To configure the pseudowire Virtual Circuit Connection Verification (VCCV) control channel (CC) type for Multiprotocol Label Switching (MPLS) pseudowires, use the **vccv** command in pseudowire class configuration mode. To disable a pseudowire VCCV CC type, use the **no** form of this command.

```
vccv { control-word | router-alert | tfl }
```

```
no vccv { control-word | router-alert | tfl }
```

Syntax Description

control-word	Specifies the control channel (CC) Type 1: control word.
router-alert	Specifies the CC Type 2: MPLS router alert label.
tfl	Specifies the CC Type 3: MPLS pseudowire label with Time to Live (TTL).

Command Default

The pseudowire VCCV CC type is set to Type 1 (control word).

Command Modes

Pseudowire-class configuration (config-pw-class)

Command History

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

Usage Guidelines

When an initiating provider edge (PE) device sends a setup request message to a remote PE device, the message includes VCCV capability information. This capability information is a combination of the CC type and the control verification (CV) type. You use the **vccv** command to configure the CC type capabilities of the MPLS pseudowire.

If the CV type for the MPLS pseudowire is set to a type that does not use IP/User Datagram Protocol (UDP) headers, then you must set the CC type to the CC Type 1: control word.

Examples

The following example shows how to configure the MPLS pseudowire class to use CC Type 1:

```
Router(config)# pseudowire-class bfdclass
Router(config-pw-class)# encapsulation mpls
Router(config-pw-class)# protocol none
Router(config-pw-class)# vccv control-word
```

Related Commands

Command	Description
bfd-template	Creates a BFD template and enters BFD configuration mode.
pseudowire-class	Specifies the name of the pseudowire class and enters pseudowire class configuration mode.

Command	Description
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 pseudowire class configuration mode. To disable status signaling, use the **no** form of this command.

vccv bfd status signaling

no vccv bfd status signaling

Syntax Description This command has no arguments or keywords.

Command Default VCCV BFD status signaling is disabled.

Command Modes Pseudowire-class configuration (config-pw-class)

Command History	Release	Modification
	15.0(1)S	This command was introduced.

Usage Guidelines Use this command to allow BFD to provide status signaling functionality that indicates the fault status of an attachment circuit (AC).

Examples The following example shows how to enable VCCV BFD status signaling for a Multiprotocol Label Switching (MPLS) pseudowire class:

```
Router(config)# pseudowire-class bfdclass
Router(config-pw-class)# encapsulation mpls
Router(config-pw-class)# protocol none
Router(config-pw-class)# vccv control-word
Router(config-pw-class)# vccv bfd template bfdtemplate raw-bfd
Router(config-pw-class)# vccv bfd status signaling
```

Related Commands	Command	Description
	bfd-template	Creates a BFD template and enters BFD configuration mode.
	pseudowire-class	Specifies the name of the pseudowire class and enters pseudowire class configuration mode.
	vccv	Configures the pseudowire VCCV CC type for MPLS pseudowires.
	vccv bfd template	Enables VCCV BFD for a pseudowire class.

vccv bfd template

To enable Virtual Circuit Connection Verification (VCCV) Bidirectional Forwarding Detection (BFD) for a pseudowire class, use the **vccv bfd template** command in pseudowire class configuration mode. To disable VCCV BFD, use the **no** form of this command.

```
vccv bfd template name [udp | raw-bfd]
```

```
no vccv bfd template name [udp | raw-bfd]
```

Syntax Description

<i>name</i>	The name of the BFD template to use.
udp	(Optional) Enables support for BFD with IP/User Datagram Protocol (UDP) header encapsulation.
raw-bfd	(Optional) Enables support for BFD without IP/UDP header encapsulation.

Command Default

VCCV BFD is not enabled for the pseudowire class.

Command Modes

Pseudowire-class configuration (config-pw-class)

Command History

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

Usage Guidelines

The BFD template specified by the *name* argument is created using the **bfd-template** command, and contains settings for the BFD interval values.

VCCV defines two types encapsulation for VCCV messages to differentiate them from data packets: BFD with IP/UDP headers and BFD without IP/UDP headers.

Support for BFD without IP/UDP headers can be enabled only for pseudowires that use a control word, or a Layer 2 Specific Sublayer (L2SS) that can take the pseudowire associated Channel Header Control Word format.

If the VCCV carries raw BFD, the control word or the L2SS Channel Type must be set to BFD without IP/UDP headers. BFD without IP/UDP headers allows the system to identify the BFD packet when demultiplexing the control channel.

Examples

The following example shows how to enable the BFD template without support for IP/UDP header encapsulation:

```
Router(config)# pseudowire-class bfdclass
Router(config-pw-class)# encapsulation mpls
Router(config-pw-class)# protocol none
Router(config-pw-class)# vccv control-word
Router(config-pw-class)# vccv bfd template bfdtemplate raw-bfd
Router(config-pw-class)# vccv bfd status signaling
```