IP Routing Protocol-Independent Commands_ S through T

send-lifetime

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

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

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

Syntax Description

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

Command Default

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

Command Modes

Key chain key configuration (config-keychain-key)

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

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

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

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

Related Commands

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

set automatic-tag

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

set automatic-tag

no set automatic-tag

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

Route-map configuration

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

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

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

set ip next-hop

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

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

no set ip next-hop {*ip-address* [*...ip-address*]| **dynamic dhcp**| **encapsulate l3vpn** *profile-name*| **peer-address**| **recursive** [**global**| **vrf** *vrf-name*] *ip-address*| **verify-availability** [*ip-address sequence* **track** *track-object-number*]}

Catalyst 3850 Switches

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

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

Syntax Description

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

track	(Optional) Sets the next hop depending on the state of a tracked object.
track-object-number	(Optional) The tracked object number. The range is from 1 to 500.

Command Default

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

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
11.0	This command was introduced.
12.0(28)S	This command was modified. The **recursive** keyword was added.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.2	In Cisco IOS XE Release 2.2, this command was integrated into the Cisco ASR 1000 Series Routers.
12.2(33)SRE	This command was modified. The **encapsulate** and **l3vpn** keywords were added.
Cisco IOS XE 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE. The **set ip next-hop** *ip-address* [...*ip-address*] command is available on Catalyst 3850 Series switches.

Usage Guidelines

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

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

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

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

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

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

Note The **set ip next-hop** command does not support Inherit-VRF routing on Cisco 7600 series routers because the **set ip next-hop** *ip-address* command is treated as equivalent to the **set ip global next-hop** *ip-address* command on Cisco 7600 series routers. (Inherit-VRF routing enables packets arriving on a VRF interface to be routed by the same outgoing interface.) Therefore, when using Cisco 7600 series routers, we recommend that you use the **set ip vrf** *vrf* **next-hop** command to explicitly indicate the VRF from which the next hop is to be chosen. We also recommend that in Cisco 7600 series routers, the **set ip next-hop** command be used only for route maps applied on non-VRF interfaces, where the software behavior and the hardware behavior would be similar.

Examples

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

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

The following example shows how IP address 10.3.3.3 is set as the recursive next-hop address:

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

Related Commands

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

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

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

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

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

Syntax Description

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

Command Default

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

Command Modes

Route-map configuration

Command History

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

Usage Guidelines

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

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

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

The **stub-areaandbackbonekeywordshavenoeffectonwhereroutesareimported.**

Examples

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

```
route-map name
 set level level-l
```

Related Commands

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

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

set local-preference

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

set local-preference *number*

no set local-preference

Syntax Description

number	Preference value. An integer from 0 to 4294967295.

Command Default

Preference value of 100

Command Modes

Route-map configuration (config-route-map)

Command History

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

Usage Guidelines

The local preference attribute is a number that indicates the relative preference of one route over another when there is more than one route to a destination. A higher preference causes a route to be preferred over a route with a lower preference.

This attribute is exchanged between iBGP peers only. That is, the preference is sent to all routers in the local autonomous system only. This attribute is used to determine local policy

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

Examples

The following example sets the local preference to 200 for all routes that are included in access list 1:

```
route-map map-preference
 match as-path 1
 set local-preference 200
```

Related Commands

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

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

set metric (BGP-OSPF-RIP)

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

set metric *metric-value*

no set metric *metric-value*

Syntax Description

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

Command Default

The dynamically learned metric value.

Command Modes

Route-map configuration (config-route-map)

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

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

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

set metric-type

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

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

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

Syntax Description

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

Command Default

This command is disabled by default.

Command Modes

Route-map configuration

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

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

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

set next-hop

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

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

no set next-hop *next-hop*

Syntax Description

next-hop	IP address of the next hop router.

Command Default

Default next hop address.

Command Modes

Route-map configuration

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

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

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

set tag (IP)

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

set tag {*tag-value*| *tag-value-dotted-decimal*}

no set tag {*tag-value*| *tag-value-dotted-decimal*}

Syntax Description

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

Command Default

Routes are not tagged.

Command Modes

Route-map configuration (config-route-map)

Command History

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

Usage Guidelines

Use the **set tag** command to set an administrative tag for a route within a route map. Route tags are 32-bit values attached to routes. You can set tag values as plain decimals or dotted decimals. Route tags are used by

route maps to filter routes. The tag value has no impact on routing decisions. It is used to mark or flag routes to prevent routing loops when routes are redistributed between routing protocols.

Examples

The following example shows how to set the tag value of the destination routing protocol to 5:

```
Device(config)# route-map tag
Device(config-route-map)# set tag 5
```

The following example shows how to set the tag value in the dotted-decimal format:

```
Device(config)# route-map tag
Device(config-route-map)# set tag 10.10.10.10
```

Related Commands

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

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

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

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

S Release	Modification
12.0(31)S	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRC	This command was modified. The **vrf** *vrf-name* keyword and argument, the **client** keyword, and the *ip-address* argument were added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was modified. The output was modified to display the "OurAddr" field only with the **details** keyword.
12.2(33)SRE	This command was modified. Support for IPv6 was added.
15.1(2)S	This command was modified. • The **show bfd neighbors details** command output was changed for hardware-offloaded BFD sessions. • The **show bfd neighbors** command output was changed to display the header type to identify the session type.
15.1(3)S	This command was modified to display information about multihop sessions.
15.2(4)S	This command was modified. The output of the command was enhanced to include Template and Authentication fields for single-hop sessions.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
15.4(3)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.
T Release	**Modification**
12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.
12.4(9)T	This command was modified. Support for BFD Version 1 and BFD echo mode was added.

S Release	Modification
15.1(2)T	This command was modified. Support for IPv6 was added.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
15.2(1)E	This command was integrated into Cisco IOS Release 15.2(1)E.
XE Release	**Modification**
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

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

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

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

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

Examples

The following is sample output from the **show bfd neighbors** that shows the status of the adjacency or neighbor:

```
Device# show bfd neighbors

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

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

```
Device# show bfd neighbors details

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

The following is sample output from the **show bfd neighbors** command when it is entered on a Cisco 12000 Series Internet Router Route Processor (RP) that shows the status of the adjacency or neighbor:

```
Device# show bfd neighbors

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

The following is sample output from the **show bfd neighbors** command when it is entered in a Cisco 12000 Series Internet Router RP that shows the status of the adjacency or neighbor with the **details** keyword:

```
Device# show bfd neighbors details

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

The following is sample output from the **show bfd neighbors** command when it is entered on a Cisco 12000 Series Internet Router line card that shows the status of the adjacency or neighbor:

```
Device# attach 6

Entering Console for 8 Port Fast Ethernet in Slot: 6
Type "exit" to end this session
Press RETURN to get started!

Device> show bfd neighbors

Cleanup timer hits: 0
OurAddr       NeighAddr     LD/RD RH  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 is sample output from the **show bfd neighbors** command when it is entered on a Cisco 12000 Series Internet Router line card that shows the status of the adjacency or neighbor with the **details** keyword:

```
Device# attach 6

Entering Console for 8 Port Fast Ethernet in Slot: 6
Type "exit" to end this session
Press RETURN to get started!
Device> show bfd neighbors details

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

```
 Total Adjs Found: 1
Device>
```

Examples

The following is sample output from the **show bfd neighbors details** command that shows that the BFD neighbor device is running BFD Version 1 and that the BFD session is up and running in echo mode:

```
Device# show bfd neighbors details

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

The following is sample output from the **show bfd neighbors** command that displays all IPv6 sessions:

```
Device# show bfd neighbors ipv6 2001::1

OurAddr                   NeighAddr                 LD/RD  RH/RS  Holddown(mult)  State
Int
2001:DB8:0:ABCD::1        2001:DB8:0:ABCD::2        2/2    Up        0    (3 )   Up
Et0/0
2001:DB8:0:1:FFFF:1234::5 2001:DB8:0:1:FFFF:1234::6 4/4    Up        0    (3 )   Up
Et1/0
```

The following is a sample output from the **show bfd neighbors**

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

```
 Device# show bfd neighbors

NeighAddr                         LD/RD    RH/RS     State     Int
192.0.2.1                          4/0     Down      Down      Et0/0
192.0.2.2                          5/0     Down      Down      Et0/0
192.0.2.3                          6/0     Down      Down      Et0/0
192.0.2.4                          7/0     Down      Down      Et0/0
192.0.2.5                          8/0     Down      Down      Et0/0
192.0.2.6                         11/0         0(RH) Fail      Et0/0
2001:DB8::1                       9/0     Down      Down      Et0/0
2001:DB8:0:ABCD::1                10/0     Down      Down      Et0/0
2001:DB8::2                        1/0         0(RH) Fail      Et0/0
2001:DB8:0:1::1                    2/0     Down      Down      Et0/0
2001:DB8:0:1:FFFF:1234::5          3/0     Down      Down      Et0/0
```

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

```
Device# show bfd neighbors details

IPv4 Sessions
NeighAddr                              LD/RD         RH/RS     State     Int
100.0.2.1                             127/156        Down      Init      Se0/5/1.1/2/1/1:0
Session Host: Hardware - session negotiated with platform adjusted timer values.
              MinTxInt - configured: 200000      adjusted: 1000000
OurAddr: 100.0.2.2
Handle: 2
Local Diag: 1, Demand mode: 0, Poll bit: 0
MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3
Received MinRxInt: 1000000, Received Multiplier: 3
Holddown (hits): 0(0), Hello (hits): 1000(0)
```

```
Rx Count: 5052
Tx Count: 7490
Elapsed time watermarks: 0 0 (last: 0)
Registered protocols: IPv4 Static CEF
Template: software
Downtime: 00:00:05
Last packet: Version: 1                  - Diagnostic: 3
             State bit: Down             - Demand bit: 0
             Poll bit: 0                 - Final bit: 0
             C bit: 1
             Multiplier: 3               - Length: 24
             My Discr.: 156              - Your Discr.: 0
             Min tx interval: 1000000    - Min rx interval: 1000000
             Min Echo interval: 200000
```

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

Table 1: 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 (LD) and remote discriminator (RD) being used for the session.
RH	Remote Heard (RH) Indicates that the remote BFD neighbor has been heard.
Holdown (mult)	Detect timer multiplier that is used for this session.
State	State of the interface—Up or Down.
Int	Interface type and slot/port.
Session state is UP and using echo function with 50 ms interval.	BFD is up and running in echo mode. The 50-millisecond interval has been adopted from the **bfd** command. **Note** BFD Version 1 and echo mode are supported only in Cisco IOS Release 12.4(9)T and later releases.
Rx Count	Number of BFD control packets that are received from the BFD neighbor.
Tx Count	Number of BFD control packets that are sent by the BFD neighbor.
Tx Interval	The interval, in milliseconds, between sent BFD packets.
Registered protocols	Routing protocols that are registered with BFD.

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

Field	Description
Final bit	Indicates that 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, it indicates that 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, it indicates that a failure has occurred.
Length	Length of the BFD control packet, in bytes.
My Discr.	My Discriminator is a unique, nonzero discriminator value generated by the transmitting system used to demultiplex multiple BFD sessions between the same pair of systems.
Your Discr.	Your Discriminator is a discriminator that is received from the corresponding remote system. This field reflects the received value of My Discriminator or is zero if that value is unknown.
Min tx interval	Minimum transmission interval, in microseconds, that the local system wants to use when sending BFD control packets.
Min rx interval	Minimum receipt interval, in microseconds, between received BFD control packets that the system can support.
Min Echo interval	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.

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

```
Device# show bfd neighbors details

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

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

```
Device# show bfd neighbors

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

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

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

```
Device# show bfd neighbors

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

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

```
Device# show bfd neighbors

IPv4 Sessions
NeighAddr                            LD/RD    RH/RS     State     Int
192.0.2.1                             6/0     Down      Down      Et1/0
203.0.113.1                           7/6     Up        Up        Et3/0
198.51.100.2                          8/7     Up        Up        Et0/0
IPv6 Sessions
NeighAddr                          LD/RD    RH/RS     State     Int
2001:DB8::1                         1/1     Up        Up        Et0/0
2001:DB8:0:ABCD::1                  2/2     Up        Up        Et0/0
2001:DB8::2                         3/3     Up        Up        Et0/0
2001:DB8:0:1:FFFF:1234::5           4/4     Up        Up        Et0/0
2001:DB8:0:1::1                     5/5     Up        Up        Et0/0
```

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

Table 2: show bfd neighbors Field Descriptions

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

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

```
Device# show bfd neighbors

IPv4 Sessions
NeighAddr                              LD/RD         RH/RS     State     Int
192.0.2.6                                1/12         Up        Up        Et0/0
Session state is UP and using echo function with 300 ms interval.
Session Host: Software
OurAddr: 192.0.2.12
Handle: 12
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3
Received MinRxInt: 1000000, Received Multiplier: 3
Holddown (hits): 0(0), Hello (hits): 1000(62244)
Rx Count: 62284, Rx Interval (ms) min/max/avg: 1/2436/878 last: 239 ms ago
Tx Count: 62247, Tx Interval (ms) min/max/avg: 1/1545/880 last: 246 ms ago
Elapsed time watermarks: 0 0 (last: 0)
Registered protocols: Stub CEF
Template: my-template
Authentication(Type/Keychain): sha-1/my-chain
Uptime: 00:22:06
Last packet: Version: 1                  - Diagnostic: 0
             State bit: Up               - Demand bit: 0
             Poll bit: 0                 - Final bit: 0
             Multiplier: 3               - Length: 24
             My Discr.: 12               - Your Discr.: 1
             Min tx interval: 1000000    - Min rx interval: 1000000
             Min Echo interval: 300000
```

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

Table 3: show bfd neighbors Field Descriptions for Single-Hop BFD Sessions

Field	Description
Template	BFD multihop template name.
Authentication	Authentication type and key chain.

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

```
Device# show bfd neighbors

IPv4 Multihop Sessions
NeighAddr[vrf]                                LD/RD         RH/RS     State
192.0.2.20                                       2/13         Up        Up
Session state is UP and not using echo function.
```

```
Session Host: Software
OurAddr: 192.0.2.21
Handle: 13
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 750000, MinRxInt: 750000, Multiplier: 3
Received MinRxInt: 750000, Received Multiplier: 15
Holddown (hits): 10772(0), Hello (hits): 750(82985)
Rx Count: 82973, Rx Interval (ms) min/max/avg: 24/1334/659 last: 478 ms ago
Tx Count: 82935, Tx Interval (ms) min/max/avg: 1/1141/660 last: 78 ms ago
Elapsed time watermarks: 0 0 (last: 0)
Registered protocols: Xconnect
Map information:
 Destination[vrf]: 192.0.2.1/24
 Source[vrf]: 192.0.2.2/24
 Template: mh
 Authentication(Type/Keychain): md5/qq
 last_tx_auth_seq: 5  last_rx_auth_seq 4
Uptime: 15:12:26
Last packet: Version: 1                  - Diagnostic: 0
             State bit: Up               - Demand bit: 0
             Poll bit: 0                 - Final bit: 0
             Multiplier: 15              - Length: 48
             My Discr.: 13               - Your Discr.: 2
             Min tx interval: 750000     - Min rx interval: 750000
             Min Echo interval: 0
```

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

Table 4: show bfd neighbors Field Descriptions for Multihop BFD Sessions

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

Related Commands

Command	Description
attach	Connects to a specific line card to execute monitoring and maintenance commands on that line card.
show bfd drops	Displays the number of dropped packets in BFD.
show bfd summary	Displays summary information for BFD.

show dampening interface

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

show dampening interface commandshow dampening interface

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC Privileged EXEC

Command History

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

Examples

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

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

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

Table 5: 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 **showinterface** dampening command in privileged EXEC mode.

show interface dampening commandshow interface dampening

Syntax Description

This command has no keywords or arguments.

Command Modes

Privileged EXEC

Command History

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

Examples

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

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

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

Table 6: show interface dampening Field Descriptions

Field	Description
Flaps	Displays the number of times that an interface has flapped.
Penalty	Displays the accumulated penalty.
Supp	Indicates if the interface is dampened.
ReuseTm	Displays the reuse timer.

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

Related Commands

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

show ip cache policy

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

show ip cache policy commandshow ip cache policy

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

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

Examples

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

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

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

Table 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 **setipnext-hop** command. “Int” indicates the **setinterface**command.
Routemap	Name of the route map that created the entry; in this example, george.
sequence	Route map sequence number.

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

Related Commands

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

show ip local policy

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

show ip local policy commandshow ip local policy

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

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

Examples

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

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

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

Table 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.

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

Related Commands

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

show ip policy

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

show ip policy

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC Privileged EXEC

Command History

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

Examples

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

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

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

```
Router# show route-map
route-map equal, permit, sequence 10
  Match clauses:
    length 150 200
  Set clauses:
    ip next-hop 10.10.11.254
  Policy routing matches: 0 packets, 0 bytes
route-map equal, permit, sequence 20
  Match clauses:
    ip address (access-lists): 101
  Set clauses:
    ip next-hop 10.10.11.14
  Policy routing matches: 144 packets, 15190 bytes
```

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

Table 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.

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

show ip protocols

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

show ip protocols commandshow ip protocols

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

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

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

Examples

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

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

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

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

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

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

Examples

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

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

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

Table 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.
Routing	Specifies the networks for which the routing process is currently injecting routes.
Routing Information Sources	Lists all the routing sources the Cisco IOS software is using to build its routing table. For each source, you will see the following displayed: • IP address • Administrative distance • Time the last update was received from this source

Examples

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

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

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

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

Table 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.

Field	Description
Default version control:	Specifies the version of RIP packets that are sent and received.
Routing	Specifies the networks for which the routing process is currently injecting routes.
Routing Information Sources	Lists all the routing sources the Cisco IOS software is using to build its routing table. For each source, you will see the following displayed: • IP address • Administrative distance • Time the last update was received from this source

Examples

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

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

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

Table 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.

Field	Description
Default networks...	Specifies how these networks will be handled in both incoming and outgoing updates.
EIGRP...	Specifies the value of the K0-K5 metrics, and the maximum hop count.
Redistributing	Lists the protocol that is being redistributed.
EIGRP NSF-Aware...	Displays the route-hold timer value.
Automatic network summarization...	Specifies that automatic summarization is enabled.
Routing	Specifies the networks for which the routing process is currently injecting routes.
Routing Information Sources	Lists all the routing sources the Cisco IOS software is using to build its routing table. For each source, you will see the following displayed: • IP address • Administrative distance • Time the last update was received from this source

Related Commands

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

show ip route

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

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

Syntax Description

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

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

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
9.2	This command was introduced.
10.0	This command was modified. The “D—EIGRP, EX—EIGRP, N1—SPF NSSA external type 1 route” and “N2—OSPF NSSA external type 2 route” codes were included in the command output.
10.3	This command was modified. The *process-id* argument was added.
11.0	This command was modified. The **longer-prefixes** keyword was added.
11.1	This command was modified. The “U—per-user static route” code was included in the command output.
11.2	This command was modified. The “o—on-demand routing” code was included in the command output.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA, and the **update-queue** keyword was added.
11.3	This command was modified. The command output was enhanced to display the origin of an IP route in Intermediate System-to-Intermediate System (IS-IS) networks.
12.0(1)T	This command was modified. The “M—mobile” code was included in the command output.
12.0(3)T	This command was modified. The “P—periodic downloaded static route” code was included in the command output.
12.0(4)T	This command was modified. The “ia—IS-IS” code was included in the command output.
12.2(2)T	This command was modified. The command output was enhanced to display information on multipaths to the specified network.

Release	Modification
12.2(13)T	This command was modified. The *egp* and *igrp* arguments were removed because the Exterior Gateway Protocol (EGP) and the Interior Gateway Routing Protocol (IGRP) were no longer available in Cisco software.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX.
12.3(2)T	This command was modified. The command output was enhanced to display route tag information.
12.3(8)T	This command was modified. The command output was enhanced to display static routes using DHCP.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRE	This command was modified. The **dhcp** and **repair-paths** keywords were added.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5. The **next-hop-override** and **nhrp** keywords were added.
15.2(2)S	This command was modified. The command output was enhanced to display route tag values in dotted decimal format.
Cisco IOS XE Release 3.6S	This command was modified. The command output was enhanced to display route tag values in dotted decimal format.
15.2(4)S	This command was implemented on the Cisco 7200 series router.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
15.4(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Examples

Examples

The following is sample output from the **show ip route** command when an IP address is not specified:

```
Device# show ip route

Codes: R - RIP derived, O - OSPF derived,
       C - connected, S - static, B - BGP derived,
```

```
       * - candidate default route, IA - OSPF inter area route,
       i - IS-IS derived, ia - IS-IS, U - per-user static route,
       o - on-demand routing, M - mobile, P - periodic downloaded static route,
       D - EIGRP, EX - EIGRP external, E1 - OSPF external type 1 route,
       E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
       N2 - OSPF NSSA external type 2 route
Gateway of last resort is 10.119.254.240 to network 10.140.0.0
O E2 10.110.0.0 [160/5] via 10.119.254.6, 0:01:00, Ethernet2
E    10.67.10.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
O E2 10.68.132.0 [160/5] via 10.119.254.6, 0:00:59, Ethernet2
O E2 10.130.0.0 [160/5] via 10.119.254.6, 0:00:59, Ethernet2
E    10.128.0.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E    10.129.0.0 [200/129] via 10.119.254.240, 0:02:22, Ethernet2
E    10.65.129.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E    10.10.0.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E    10.75.139.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
E    10.16.208.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E    10.84.148.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
E    10.31.223.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E    10.44.236.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
E    10.141.0.0 [200/129] via 10.119.254.240, 0:02:22, Ethernet2
E    10.140.0.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
```

The following sample output from the **show ip route** command includes routes learned from IS-IS Level 2:

```
Device# show ip route

Codes: R - RIP derived, O - OSPF derived,
       C - connected, S - static, B - BGP derived,
       * - candidate default route, IA - OSPF inter area route,
       i - IS-IS derived, ia - IS-IS, U - per-user static route,
       o - on-demand routing, M - mobile, P - periodic downloaded static route,
       D - EIGRP, EX - EIGRP external, E1 - OSPF external type 1 route,
       E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
       N2 - OSPF NSSA external type 2 route
Gateway of last resort is not set
     10.89.0.0 is subnetted (mask is 255.255.255.0), 3 subnets
C       10.89.64.0 255.255.255.0 is possibly down,
          routing via 10.0.0.0, Ethernet0
i L2    10.89.67.0 [115/20] via 10.89.64.240, 0:00:12, Ethernet0
i L2    10.89.66.0 [115/20] via 10.89.64.240, 0:00:12, Ethernet0
```

The following is sample output from the **show ip route** *ip-address mask* **longer-prefixes** command. When this keyword is included, the address-mask pair becomes the prefix, and any address that matches that prefix is displayed. Therefore, multiple addresses are displayed. The logical AND operation is performed on the source address 10.0.0.0 and the mask 10.0.0.0, resulting in 10.0.0.0. Each destination in the routing table is also logically ANDed with the mask and compared with 10.0.0.0. Any destinations that fall into that range are displayed in the output.

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

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

Gateway of last resort is not set

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

```
S    10.44.237.0 is directly connected, Ethernet0
S    10.31.222.0 is directly connected, Ethernet0
S    10.16.209.0 is directly connected, Ethernet0
S    10.145.0.0 is directly connected, Ethernet0
S    10.141.0.0 is directly connected, Ethernet0
S    10.138.0.0 is directly connected, Ethernet0
S    10.128.0.0 is directly connected, Ethernet0
     10.19.0.0 255.255.255.0 is subnetted, 1 subnets
C       10.19.64.0 is directly connected, Ethernet0
     10.69.0.0 is variably subnetted, 2 subnets, 2 masks
C       10.69.232.32 255.255.255.240 is directly connected, Ethernet0
S       10.69.0.0 255.255.0.0 is directly connected, Ethernet0
```

The following sample outputs from the **show ip route** command display all downloaded static routes. A “p” indicates that these routes were installed using the AAA route download function.

```
Device# show ip route

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

Gateway of last resort is 172.16.17.1 to network 10.0.0.0

        172.31.0.0/32 is subnetted, 1 subnets
P       172.31.229.41 is directly connected, Dialer1 10.0.0.0/8 is subnetted, 3 subnets
P       10.1.1.0 [200/0] via 172.31.229.41, Dialer1
P       10.1.3.0 [200/0] via 172.31.229.41, Dialer1
P       10.1.2.0 [200/0] via 172.31.229.41, Dialer1

Device# show ip route static

     172.16.4.0/8 is variably subnetted, 2 subnets, 2 masks
P       172.16.1.1/32 is directly connected, BRI0
P       172.16.4.0/8 [1/0] via 10.1.1.1, BRI0
S    172.31.0.0/16 [1/0] via 172.16.114.65, Ethernet0
S    10.0.0.0/8 is directly connected, BRI0
P    10.0.0.0/8 is directly connected, BRI0
     172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
S       172.16.114.201/32 is directly connected, BRI0
S       172.16.114.205/32 is directly connected, BRI0
S       172.16.114.174/32 is directly connected, BRI0
S       172.16.114.12/32 is directly connected, BRI0
P    10.0.0.0/8 is directly connected, BRI0
P    10.1.0.0/16 is directly connected, BRI0
P    10.2.2.0/24 is directly connected, BRI0
S*   0.0.0.0/0 [1/0] via 172.16.114.65, Ethernet0
S    172.16.0.0/16 [1/0] via 172.16.114.65, Ethernet0
```

The following sample output from the **show ip route static download** command displays all active and inactive routes installed using the AAA route download function:

```
Device# show ip route static download

Connectivity: A - Active, I - Inactive

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

The following sample outputs from the **show ip route nhrp** command display shortcut switching on the tunnel interface:

```
Device# show ip route

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

Device# show ip route nhrp

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

The following are sample outputs from the **show ip route** command when the **next-hop-override** keyword is used. When this keyword is included, the NHRP next-hop overrides that are associated with a particular route and the corresponding default next hops are displayed.

```
================================================================
1) Initial configuration
================================================================

Device# show ip route

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

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

Device# show ip route next-hop-override

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

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

```
S        10.11.11.0 is directly connected, Ethernet0/0

Device# show ip cef

Prefix               Next Hop             Interface
.
.
.
10.2.1.255/32         receive              Loopback1
10.10.10.0/24        attached             Tunnel0  <<<<<<<<
10.11.11.0/24        attached             Ethernet0/0
172.16.0.0/12          drop
.
.
.
================================================================
2) Add a next-hop override
   address = 10.10.10.0
   mask = 255.255.255.0
   gateway = 10.1.1.1
   interface = Tunnel0
================================================================

Device# show ip route

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

Gateway of last resort is not set
      10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        10.2.1.0/24 is directly connected, Loopback1
L        10.2.1.1/32 is directly connected, Loopback1
      10.0.0.0/24 is subnetted, 1 subnets

S        10.10.10.0 is directly connected, Tunnel0
      10.11.0.0/24 is subnetted, 1 subnets
S        10.11.11.0 is directly connected, Ethernet0/0

Device# show ip route next-hop-override

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

Gateway of last resort is not set
      10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        10.2.1.0/24 is directly connected, Loopback1
L        10.2.1.1/32 is directly connected, Loopback1
      10.0.0.0/24 is subnetted, 1 subnets

S        10.10.10.0 is directly connected, Tunnel0
                  [NHO][1/0] via 10.1.1.1, Tunnel0
      10.11.0.0/24 is subnetted, 1 subnets
S        10.11.11.0 is directly connected, Ethernet0/0

Device# show ip cef

Prefix               Next Hop             Interface
.
.
.
10.2.1.255/32         receive              Loopback110.10.10.0/24
```

```
10.10.10.0/24       10.1.1.1              Tunnel0

10.11.11.0/24       attached            Ethernet0/0
10.12.0.0/16 drop
.
.
.
==============================================================
3) Delete a next-hop override
   address = 10.10.10.0
   mask = 255.255.255.0
   gateway = 10.11.1.1
   interface = Tunnel0
==============================================================

Device# show ip route

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

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

Device# show ip route next-hop-override

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

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

Device# show ip cef

Prefix               Next Hop             Interface
.
.
.
10.2.1.255/32         receive              Loopback110.10.10.0/24

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

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

Table 14: show ip route Field Descriptions

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

Field	Description
10.110.0.0	Indicates the address of the remote network.
[160/5]	The first number in brackets is the administrative distance of the information source; the second number is the metric for the route.
via 10.119.254.6	Specifies the address of the next device to the remote network.
0:01:00	Specifies the last time the route was updated (in hours:minutes:seconds).
Ethernet2	Specifies the interface through which the specified network can be reached.

Examples

The following is sample output from the **show ip route** command when an IP address is specified:

```
Device# show ip route 10.0.0.1

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

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

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

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

Table 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.
Redistributing via...	Indicates the redistribution protocol.

Field	Description
Last update from 10.191.255.251	Indicates the IP address of the router that is the next hop to the remote network and the interface on which the last update arrived.
Routing Descriptor Blocks	Displays the next-hop IP address followed by the information source.
Route metric	This value is the best metric for this Routing Descriptor Block.
traffic share count	Indicates the number of packets transmitted over various routes.

The following sample output from the **show ip route** command displays the tag applied to the route 10.22.0.0/16. You must specify an IP prefix to see the tag value. The fields in the display are self-explanatory.

```
Device# show ip route 10.22.0.0

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

Examples

The following example shows that IP route 10.8.8.0 is directly connected to the Internet and is the next-hop (option 3) default gateway. Routes 10.1.1.1 [1/0], 10.3.2.1 [24/0], and 172.16.2.2 [1/0] are static, and route 10.0.0.0/0 is a default route candidate. The fields in the display are self-explanatory.

```
Device# show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is 10.0.19.14 to network 0.0.0.0
10.0.0.0/24 is subnetted, 1 subnets
C 10.8.8.0 is directly connected, Ethernet1
  10.0.0.0/32 is subnetted, 1 subnets
S 10.1.1.1 [1/0] via 10.8.8.1
  10.0.0.0/32 is subnetted, 1 subnets
S 10.3.2.1 [24/0] via 10.8.8.1
  172.16.0.0/32 is subnetted, 1 subnets
S 172.16.2.2 [1/0] via 10.8.8.1
  10.0.0.0/28 is subnetted, 1 subnets
C 10.0.19.0 is directly connected, Ethernet0
  10.0.0.0/24 is subnetted, 1 subnets
C 10.15.15.0 is directly connected, Loopback0
S* 10.0.0.0/0 [1/0] via 10.0.19.14
```

The following sample output from the **show ip route repair-paths** command shows repair paths marked with the tag [RPR]. The fields in the display are self-explanatory:

```
Device# show ip route repair-paths

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

Gateway of last resort is not set

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

Device# show ip route repair-paths 10.9.9.9

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

Related Commands

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

show ip route summary

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

shshow ip route summary commandow ip route summary

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

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

Examples

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

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

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

Table 16: show ip route summary Field Descriptions

Field	Description
IP routing table name is...	Displays routing table type and table ID.
IP routing table maximum-paths is...	Number of parallel routes supported by this routing table.

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

show ip route supernets-only

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

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

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

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

Examples

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

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

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

Table 17: show ip route supernets-only Field Descriptions

Field	Description
B	Border Gateway Protocol (BGP) derived, as shown in list of codes.
172.16.0.0 (mask is 255.255.0.0)	Supernet IP address.
[20/0]	Administrative distance (external/internal).

Field	Description
via 172.16.72.30	Next hop IP address.
0:00:50	Age of the route (how long ago the update was received).

show ipv6 route

To display contents of the IPv6 routing table, use the **show ipv6 route** command in user EXEC or privileged EXEC mode.

show ipv6 route [*ipv6-address*| *ipv6-prefix*/*prefix-length* [**longer-prefixes**]| [*protocol*] | [**repair**] | [**updated** [**boot-up**] [*day month*] [*time*]]| **interface** *type number*| **nd**| **nsf**| **table** *table-id* | **watch**]

Syntax Description

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

nsf	(Optional) Displays routes in the nonstop forwarding (NSF) state.
repair	(Optional)
table *table-id*	(Optional) Displays IPv6 RIB table information for the specified table ID. The table ID must be in hexadecimal format. The range is from 0 to 0-0xFFFFFFFF.
watch	(Optional) Displays information about route watchers.

Command Default

If none of the optional syntax elements is chosen, all IPv6 routing information for all active routing tables is displayed.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(8)T	This command was modified. The **isis** keyword was added, and the I1 - ISIS L1, I2 - ISIS L2, and IA - ISIS interarea fields were included in the command output.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S. The timer information was removed, and an indicator was added to display IPv6 Multiprotocol Label Switching (MPLS) interfaces.
12.2(13)T	This command was modified. The timer information was removed, and an indicator was added to display IPv6 MPLS virtual interfaces.
12.2(14)S	This command was modified. The **longer-prefixes** keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Release	Modification
Cisco IOS XE Release 2.1	This command was implemented on Cisco ASR 1000 Series Aggregation Services Routers.
12.4(24)T	This command was modified in a release earlier than Cisco IOS Release 12.4(24)T. The **table**, **nsf**, **watch**, and **updated** keywords and the *day, month, table-id*, and *time* arguments were added.
15.2(2)S	This command was modified. The command output was enhanced to include route tag values in dotted-decimal format.
Cisco IOS XE Release 3.6S	This command was modified. The command output was enhanced to include route tag values in dotted-decimal format.
15.1(1)SY	The **nd** keyword was added.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.
15.2(2)SA2	This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches.

Usage Guidelines

The **show ipv6 route** command provides output similar to the **show ip route** command, except that the information is IPv6-specific.

When the *ipv6-address* or *ipv6-prefix*/*prefix-length* argument is specified, the longest match lookup is performed from the routing table, and only route information for that address or network is displayed. When a routing protocol is specified, only routes for that protocol are displayed. When the **connected**, **local**, **mobile**, or **static** keyword is specified, only the specified type of route is displayed. When the **interface** keyword and *type* and *number* arguments are specified, only routes for the specified interface are displayed.

Examples

The following is sample output from the **show ipv6 route** command when no keywords or arguments are specified:

```
Device# show ipv6 route

IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       I1 - ISIS L1, I2 - ISIS L2, IA - IIS interarea
B   2001:DB8:4::2/48 [20/0]
     via FE80::A8BB:CCFF:FE02:8B00, Serial6/0
L   2001:DB8:4::3/48 [0/0]
     via ::, Ethernet1/0
C   2001:DB8:4::4/48 [0/0]
     via ::, Ethernet1/0
LC  2001:DB8:4::5/48 [0/0]
     via ::, Loopback0
L   2001:DB8:4::6/48 [0/0]
     via ::, Serial6/0
C   2001:DB8:4::7/48 [0/0]
     via ::, Serial6/0
S   2001:DB8:4::8/48 [1/0]
     via 2001:DB8:1::1, Null
L   FE80::/10 [0/0]
     via ::, Null0
```

```
L   FF00::/8 [0/0]
     via ::, Null0
```

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

Table 18: show ipv6 route Field Descriptions

Field	Description
Codes:	Indicates the protocol that derived the route. Values are as follows: • B—BGP derived • C—Connected • I1—ISIS L1—Integrated IS-IS Level 1 derived • I2—ISIS L2—Integrated IS-IS Level 2 derived • IA—ISIS interarea—Integrated IS-IS interarea derived • L—Local • R—RIP derived • S—Static
2001:DB8:4::2/48	Indicates the IPv6 prefix of the remote network.
[20/0]	The first number in brackets is the administrative distance of the information source; the second number is the metric for the route.
via FE80::A8BB:CCFF:FE02:8B00	Specifies the address of the next device to the remote network.

When the *ipv6-address* or *ipv6-prefix*/*prefix-length* argument is specified, only route information for that address or network is displayed. The following is sample output from the **show ipv6 route** command when IPv6 prefix 2001:DB8::/35 is specified. The fields in the display are self-explanatory.

```
Device# show ipv6 route 2001:DB8::/35

IPv6 Routing Table - 261 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
B 2001:DB8::/35 [20/3]
  via FE80::60:5C59:9E00:16, Tunnel1
```

When you specify a protocol, only routes for that particular routing protocol are shown. The following is sample output from the **show ipv6 route bgp** command. The fields in the display are self-explanatory.

```
Device# show ipv6 route bgp

IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
```

```
B   2001:DB8:4::4/64 [20/0]
     via FE80::A8BB:CCFF:FE02:8B00, Serial6/0
```

The following is sample output from the **show ipv6 route local** command. The fields in the display are self-explanatory.

```
Device# show ipv6 route local

IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
L   2001:DB8:4::2/128 [0/0]
     via ::, Ethernet1/0
LC  2001:DB8:4::1/128 [0/0]
     via ::, Loopback0
L   2001:DB8:4::3/128 [0/0]
     via ::, Serial6/0
L   FE80::/10 [0/0]
     via ::, Null0
L   FF00::/8 [0/0]
     via ::, Null0
```

The following is sample output from the **show ipv6 route** command when the 6PE multipath feature is enabled. The fields in the display are self-explanatory.

```
Device# show ipv6 route

IPv6 Routing Table - default - 19 entries
Codes:C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
.
.
.
B   2001:DB8::/64 [200/0]
     via ::FFFF:172.16.0.1
     via ::FFFF:172.30.30.1
```

Related Commands

Command	Description
ipv6 route	Establishes a static IPv6 route.
show ipv6 interface	Displays IPv6 interface information.
show ipv6 route summary	Displays the current contents of the IPv6 routing table in summary format.
show ipv6 tunnel	Displays IPv6 tunnel information.

show key chain

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

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

Syntax Description

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

Command Default

Information about all key chains is displayed.

Command Modes

EXEC

Command History

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

Examples

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

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

Related Commands

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

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

show route-map

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

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

Syntax Description

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

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S, and support for Continue clauses was included in the command output.
12.2(27)SBA	This command was modified. The output was enhanced to display dynamically assigned route maps in VPN routing and forwarding (VRF) tables.
12.2(15)T	This command was modified. An additional counter-collect policy routing statistic was added to the command output.
12.3(2)T	This command was modified. Support for Continue clauses was included in the command output.
12.2(17b)SXA	This command was integrated into Cisco IOS Release 12.2(17b)SXA.

Release	Modification
12.3(7)T	This command was modified. The **dynamic**, **application**, and **all** keywords were added.
12.0(28)S	This command was modified. Support for the recursive next-hop clause was added to the command output.
12.3(14)T	This command was modified. Support for the recursive next-hop clause, map display extension functionality, and the **detailed** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2.
15.0(1)M	This command was modified. The **detailed** keyword was removed.
15.2(2)S	This command was modified. The command output was enhanced to display route tag values in dotted-decimal format.
Cisco IOS XE Release 3.6S	This command was modified. The command output was enhanced to display route tag values in dotted-decimal format.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

The **show route-map** command displays information about route maps configured on the router. The output will vary depending on the keywords included with the command and the Cisco software image running on your router.

Examples

Examples

The following is sample output from the **show route-map** command when no keywords or arguments are used:

```
Device# show route-map

route-map ROUTE-MAP-NAME, permit, sequence 10
  Match clauses:
    ip address (access-lists): 1
    metric 10
  Continue: sequence 40
  Set clauses:
    as-path prepend 10
  Policy routing matches: 0 packets, 0 bytes
route-map ROUTE-MAP-NAME, permit, sequence 20
  Match clauses:
    ip address (access-lists): 2
    metric 20
  Set clauses:
    as-path prepend 10 10
  Policy routing matches: 0 packets, 0 bytes
route-map ROUTE-MAP-NAME, permit, sequence 30
  Match clauses:
  Continue: to next entry 40
```

```
  Set clauses:
    as-path prepend 10 10 10
  Policy routing matches: 0 packets, 0 bytes
route-map ROUTE-MAP-NAME, deny, sequence 40
  Match clauses:
    community (community-list filter): 20:2
  Set clauses:
    local-preference 100
  Policy routing matches: 0 packets, 0 bytes
route-map LOCAL-POLICY-MAP, permit, sequence 10
  Match clauses:
  Set clauses:
    community 655370
  Policy routing matches: 0 packets, 0 bytes
```

The following sample output from the **show route-map** command displays information about route tags:

```
Device# show route-map

route-map STATIC, permit, sequence 10
  Match clauses:
    ip address (access-lists): 1
  Set clauses:
    metric 56 100 255 1 1500
    tag 1.1.1.1
  Policy routing matches: 0 packets, 0 bytes
route-map STATIC, permit, sequence 20
  Match clauses:
    ip address (access-lists): 2
  Set clauses:
    metric 56 100 255 1 1500
    tag 1.1.1.2
  Policy routing matches: 0 packets, 0 bytes
```

The following sample output from the **show route-map** command shows Multiprotocol Label Switching (MPLS)-related route map information:

```
Device# show route-map

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

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

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

```
Device# show route-map dynamic

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

```
  Set clauses:
    ip next-hop 172.16.1.1
    ip gateway 172.16.1.1
  Policy routing matches: 0 packets, 0 bytes
Current active dynamic routemaps = 1
```

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

```
Device# show route-map dynamic application

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

When you specify an application name, dynamic routes for that application are displayed. The following is sample output from the **show route-map dynamic application** command when you specify the name of the application:

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

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

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

route-map AAA-02/06/04-14:34:09.735-2-AppSpec, permit, sequence 0, identifier 1128046100
  Match clauses:
    ip address (access-lists): PBR#7 PBR#8
  Set clauses:
  Policy routing matches: 0 packets, 0 bytes
route-map AAA-02/06/04-14:34:09.735-2-AppSpec, permit, sequence 1, identifier 1141277624
  Match clauses:
    ip address (access-lists): PBR#9 PBR#10
  Set clauses:
  Policy routing matches: 0 packets, 0 bytes
route-map AAA-02/06/04-14:34:09.735-2-AppSpec, permit, sequence 2, identifier 1141279420
  Match clauses:
    ip address (access-lists): PBR#11 PBR#12
    length 10 100
  Set clauses:
    ip next-hop 172.16.1.12
    ip gateway 172.16.1.12
  Policy routing matches: 0 packets, 0 bytes
Current active dynamic routemaps = 2
```

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

```
Device# show route-map dynamic detailed

route-map AAA-01/20/04-22:03:10.799-1-AppSpec, permit, sequence 1, identifier 29675368
Match clauses:
ip address (access-lists):
Extended IP access list PBR#3
1 permit icmp 0.0.16.12 1.204.167.240 10.1.1.0 0.0.0.255 syn dscp af12 log-input fragments

Extended IP access list PBR#4
1 permit icmp 0.0.16.12 1.204.167.240 10.1.1.0 0.0.0.255 syn dscp af12 log-input fragments

Set clauses:
ip next-hop 172.16.1.14
ip gateway 172.16.1.14
Policy routing matches: 0 packets, 0 bytes
```

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

```
Device# show route-map dynamic

route-map None-06/01/04-21:14:21.407-1-IP VRF, permit, sequence 0
identifier 1675771000
```

```
 Match clauses:
 Set clauses: vrf vrf1
 Policy routing matches: 0 packets, 0 bytes
Current active dynamic routemaps = 1
```

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

Table 19: show route-map Field Descriptions

Field	Description
Route-map ROUTE-MAP-NAME	Name of the route map.
Permit	Indicates that the route is redistributed based on set actions.
Sequence	Number that indicates the position of the new route map in the list of configured route maps.
Match clauses	Match criteria or conditions based on which the route map is redistributed.
Continue	Displays the configuration of a continue clause and the next route-map entry to which the clause is sent.
Set clauses	Specific redistribution actions to be performed if the **match** command criteria are met.
Tag	Tag for routes to the remote network.
Policy routing matches	Number of packets and bytes that have been filtered by policy routing.

Related Commands

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