IP Routing Protocol-Independent Commands

accept-lifetime

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

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

no accept-lifetime [*start-time* {**infinite** | *end-time* | **duration** *seconds*}]

Syntax Description

start-time	Beginning time that the key specified by the **key** command is valid to be received. The syntax can be either of the following: *hh*:*mm*:*ss Month date year* *hh*:*mm*:*ss date Month year* *hh*—hours *mm*—minutes *ss*—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 received from the *start-time* value on.
end-time	Key is valid to be received from the *start-time* value until the *end-time* value. The syntax is the same as that for the *start-time* value. The *end-time* value must be after the *start-time* value. The default end time is an infinite time period.
duration *seconds*	Length of time (in seconds) that the key is valid to be received. The range is from 1 to 2147483646.

Command Default

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

Command Modes

Key chain key configuration

Command History

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

Usage Guidelines

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

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

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

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

Examples

The following example configures a key chain called keychain1. The key named string1 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 string2 will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or discrepancies in the set time of the router. There is a 30-minute leeway on each side to handle time differences.

```
interface ethernet 0
 ip rip authentication key-chain keychain1
 ip rip authentication mode md5
!
router rip
 network 172.19.0.0
 version 2
!
key chain keychain1
 key 1
 key-string string1
 accept-lifetime 13:30:00 Jan 25 1996 duration 7200
 send-lifetime 14:00:00 Jan 25 1996 duration 3600
 key 2
 key-string string2
 accept-lifetime 14:30:00 Jan 25 1996 duration 7200
 send-lifetime 15:00:00 Jan 25 1996 duration 3600
```

Related Commands

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

bfd

To set the baseline Bidirectional Forwarding Detection (BFD) session parameters on an interface, use the **bfd** command in interface configuration mode. To remove the baseline BFD session parameters, use the **no** form of this command.

bfd interval *milliseconds* **min_rx** *milliseconds* **multiplier** *multiplier-value*

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

Syntax Description

interval *milliseconds*	Specifies the rate at which BFD control packets will be sent to BFD peers. The configurable time period for the *milliseconds* argument is from 50 to 999 milliseconds (ms).
min_rx *milliseconds*	Specifies the rate at which BFD control packets will be expected to be received from BFD peers. The configurable time period for the *milliseconds* argument is from 50 to 999 ms.
multiplier *multiplier-value*	Specifies the number of consecutive BFD control packets that must be missed from a BFD peer before BFD declares that the peer is unavailable and the Layer 3 BFD peer is informed of the failure. The configurable value range for the *multiplier-value* argument is from 3 to 50.

Command Default

No baseline BFD session parameters are set.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)SXE	This command was introduced.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S.
12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	This command was implemented on Cisco ASR 1000 Series Aggregation Services Routers.
12.2(33)SRE	This command was modified. Support for IPv6 was added.
15.0(1)M	This command was modified. Support was removed from ATM and inverse multiplexing over ATM (IMA) interfaces.

Usage Guidelines

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

- ATM
- Dot1Q VLAN subinterfaces (with an IP address on the Dot1Q subinterface)

- Ethernet
- Frame Relay
- IMA
- PoS
- Serial

Other interface types are not supported by BFD.

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

Examples

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

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

Related Commands

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

bfd all-interfaces

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

bfd all-interfaces

no bfd all-interfaces

Syntax Description

This command has no arguments or keywords.

Command Default

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

Command Modes

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

Command History

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

Usage Guidelines

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

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

Examples

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

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

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

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

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

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

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

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

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

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

Related Commands

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

bfd echo

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

bfd echo

no bfd echo

Syntax Description

This command has no arguments or keywords.

Command Default

BFD echo mode is enabled by default.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

Echo mode is enabled by default. Entering the **no bfd echo** command without any keywords turns off the sending of echo packets and signifies that the router is unwilling to forward echo packets received from BFD neighbor routers.

When echo mode is enabled, the desired minimum echo transmit interval and required minimum transmit interval values are taken from the **bfd interval** *milliseconds* **min_rx** *milliseconds* parameters, respectively.

Note If the **no ip route-cache same-interface** command is configured, the **bfd echo accept** command will not be accepted.

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

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

Echo Mode Without Asymmetry

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

Examples

The following example configures echo mode between BFD neighbors:

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

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

```
Router# show bfd neighbors details

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

Related Commands

Command	Description
bfd	Sets the baseline BFD session parameters on the interface.
ip redirects	Enables the sending of ICMP redirect messages if the Cisco IOS software is forced to resend a packet through the same interface on which it was received.
ip route-cache	Controls the use of switching methods for forwarding IP packets.

bfd interface

To enable Bidirectional Forwarding Detection (BFD) on a per-interface basis for a BFD peer, use the **bfd interface** command in router configuration mode. To disable BFD on a per-interface basis, use the **no** form of this command.

bfd interface *type number*

no bfd interface *type number*

Syntax Description

type	Interface type for the interface to be enabled for BFD.
number	Interface number for the interface to be enabled for BFD.

Command Default

BFD is not enabled on the interface.

Command Modes

Router configuration

Command History

Release	Modification
12.2(18)SXE	This command was introduced.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S.
12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

There are two methods to configure routing protocols to use BFD for failure detection. To enable BFD for all neighbors of a routing protocol, enter the **bfd all-interfaces** command in router configuration mode. If you do not want to enable BFD on all interfaces, enter the **bfd interface** command in router configuration mode.

Examples

The following example shows BFD enabled for the Enhanced Interior Gateway Routing Protocol (EIGRP) neighbor Fast Ethernet interface 3/0:

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

Related Commands

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

bfd slow-timers

To configure the Bidirectional Forwarding Detection (BFD) slow timers value, use the **bfd slow-timers** command in global configuration mode. This command does not have a **no** form.

bfd slow-timers [*milliseconds*]

Syntax Description

milliseconds	(Optional) BFD slow timers value, in milliseconds. The range is from 1000 to 30000. The default is 1000.

Command Default

The BFD slow timer value is 1000 milliseconds.

Command Modes

Global configuration (config)

Command History

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

Examples

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

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

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

```
Router# show bfd neighbors details

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

```
Min tx interval: 14000 - Min rx interval: 14000
Min Echo interval: 4000
```

Related Commands

Command	Description
bfd echo	Enables BFD echo mode.

bfd-template

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

bfd-template single-hop *template-name*

no bfd-template single-hop *template-name*

Syntax Description

single-hop	Specifies a single-hop BFD template.
template-name	The template name.

Command Default

The BFD template does not exist.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

Command	Description
bfd	Set the baseline BFD session parameters on an interface.
bfd all-interfaces	Enables BFD for all interfaces participating in the routing process.
bfd echo	Enables BFD echo mode.
bfd interface	Enables BFD on a per-interface basis for a BFD peer.
bfd slow-timer	Configures the BFD slow timer value.
interval	Configures the transmit and receive intervals between BFD packets.

dampening

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

dampening [*half-life-period reuse-threshold*] [*suppress-threshold max-suppress-time* [*restart-penalty*]]

no dampening

Syntax Description

half-life-period	(optional) Time (in seconds) after which a penalty is decreased. Once the route has been assigned a penalty, the penalty is decreased by half after the half-life period expires. The range of the half-life period is from 1 to 30 seconds. The default time is 5 seconds.
reuse-threshold	(optional) Reuse value based on the number of penalties. When the accumulated penalty decreases enough to fall below this value, the route is unsuppressed. The range of the reuse value is from 1 to 20000; the default is 1000.
suppress-threshold	(optional) Value of the accumulated penalty that triggers the router to dampen a flapping interface.A route is suppressed when its penalty exceeds this limit. The range is from 1 to 20000; the default is 2000.
max-suppress-time	(optional) Maximum time (in seconds) a route can be suppressed. The range is from 1 to 20000; the default is four times the *half-life-period value*. If the *half-life-period* value is allowed to default, the maximum suppress time defaults to 20 seconds.
restart-penalty	(optional) Penalty to applied to the interface when it comes up for the first time after the router reloads. The configurable range is from 1 to 20000 penalties. The default is 2000 penalties. This argument is not required for any other configurations.

Defaults

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

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

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

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

Examples

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

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

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

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

Related Commands

Command	Description
clear counters	Clears the interface counters.
show dampening interface	Displays a summary of interface dampening.
show interface dampening	Displays a summary of the dampening parameters and status.

distance (IP)

To define an administrative distance for routes that are inserted into the routing table, use the **distance** command in router configuration mode. To return the administrative distance to its default distance definition, use the **no** form of this command.

distance *distance ip-address wildcard-mask* [*ip-standard-acl* | *ip-extended-acl* | *access-list-name*]

no distance *distance ip-address wildcard-mask* [*ip-standard-acl* | *ip-extended-acl* | *access-list-name*]

Syntax Description

distance	Administrative distance. An integer from 10 to 255. (The values 0 to 9 are reserved for internal use. Routes with a distance value of 255 are not installed in the routing table.)
ip-address	IP address in four-part, dotted decimal notation. The IP address or the network address from where routes are learned.
wildcard-mask	Wildcard mask in four-part, dotted decimal notation. A bit set to 1 in the *wildcard-mask* argument instructs the software to ignore the corresponding bit in the address value.
ip-standard-acl	(Optional) Standard IP access list (ACL) number to be applied to incoming routing updates.
ip-extended-acl	(Optional) Extended IP access list to be applied to incoming routing updates.
access-list-name	(Optional) Named access list to be applied to incoming routing updates.

Command Default

For information on default administrative distances, see the "Usage Guidelines" section.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
10.0	This command was introduced.
11.2	This command was modified. The *access-list-name* argument was added.
11.3	This command was modified. The **ip** keyword was removed.
12.0	This command was modified. The *ip-standard-acl* and *ip-extended-acl* arguments were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Release	Modification
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.0(1)M	This command was integrated into a release earlier than Cisco IOS Release 15.0(1)M.

Usage Guidelines

Table 1 lists default administrative distances.

Table 1 Default Administrative Distances

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

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

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

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

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

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

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

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

Examples

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

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

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

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

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

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

```
Router# show ip protocols
.
.
.
Routing Protocol is "isis tag1"
  Invalid after 0 seconds, hold down 0, flushed after 0
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Redistributing: isis
  Address Summarization:
    None
  Maximum path: 4
  Routing for Networks:
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: (default is 115)
    Address         Wild mask       Distance  List
    10.11.0.0             0.0.0.255       45
    10.0.0.0              0.0.0.255       22
    Address         Wild mask       Distance  List
    10.11.0.0             0.0.0.255       33
    10.11.12.0            0.0.0.255       44
```

Related Commands

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

distribute-list in (IP)

To filter networks received in updates, use the **distribute-list in** command in the appropriate configuration mode. To change or cancel the filter, use the **no** form of this command.

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

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

Syntax Description

access-list-number | *name*	(Optional) Standard IP access list number or name. The list defines which networks are to be received and which are to be suppressed in routing updates.
route-map *map-tag*	(Optional) Name of the route map that defines which networks are to be installed in the routing table and which are to be filtered from the routing table. This argument is supported by OSPF and EIGRP.
in	Applies the access list to incoming routing updates.
interface-type	(Optional) Interface type. The *interface-type* argument cannot be used in address family configuration mode.
interface-number	(Optional) Interface number on which the access list should be applied to incoming updates. If no interface is specified, the access list will be applied to all incoming updates. The interface *type* and *number* arguments can apply if you specify an access list, not a route map. The *interface-number* argument cannot be used in address family configuration mode.

Defaults

This command is disabled by default.

Command Modes

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

Command History

Release	Modification
10.0	This command was introduced.
11.2	The *access-list-name*, *type*, and *number* arguments were added.
12.0(7)T	Address family configuration mode was added.
12.0(24)S	The **route-map** *map-tag* keyword and argument were added.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2(33)SRB	This command was made available in router address family topology configuration mode.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

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

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

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

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

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

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

Release 12.2(33)SRB

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

Examples

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

```
access-list 1 permit 0.0.0.0
access-list 1 permit 10.108.0.0
access-list 1 deny 0.0.0.0 255.255.255.255
router eigrp 1
 network 10.108.0.0
 distribute-list 1 in
```

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

```
route-map tag-filter deny 10
 match tag 777
route-map tag-filter permit 20
```

```
!
router ospf 1
 router-id 10.0.0.2
 log-adjacency-changes
 network 172.16.2.1 0.0.0.255 area 0
 distribute-list route-map tag-filter in
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
access-list (IP standard)	Defines a standard IP access list.
distribute-list out (IP)	Suppresses networks from being advertised in updates.
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.

distribute-list out (IP)

To suppress networks from being advertised in updates, use the **distribute-list out** command in the appropriate configuration mode. To cancel this function, use the **no** form of this command.

distribute-list {*access-list-number* | *access-list-name*} **out** [*interface-name* | *routing-process* | *as-number*]

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

Syntax Description

access-list-number | *access-list-name*	Standard IP access list number or name. The list defines which networks are to be sent and which are to be suppressed in routing updates.
out	Applies the access list to outgoing routing updates.
interface-name	(Optional) Name of a particular interface. The *interface-name* argument cannot be used in address family configuration mode.
routing-process	(Optional) Name of a particular routing process, or the **static** or **connected** keyword.
as-number	(Optional) Autonomous system number.

Defaults

This command is disabled by default. Networks are advertised in updates.

Command Modes

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

Command History

Release	Modification
10.0	This command was introduced.
11.2	The *access-list-name* argument was added.
12.0(7)T	Address family configuration mode was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was made available in router address family topology configuration mode.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When networks are redistributed, a routing process name can be specified as an optional trailing argument to the **distribute-list** command. Specifying this option causes the access list to be applied to only those routes derived from the specified routing process. After the process-specific access list is

applied, any access list specified by a **distribute-list** command without a process name argument will be applied. Addresses not specified in the **distribute-list** command will not be advertised in outgoing routing updates.

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

Note To filter networks received in updates, use the **distribute-list in** command.

Release 12.2(33)SRB

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

Examples

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

```
access-list 1 permit 10.108.0.0
access-list 1 deny 0.0.0.0 255.255.255.255
router rip
 network 10.108.0.0
 distribute-list 1 out
```

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

```
router eigrp 100
 distribute-list 1 out
access-list 1 permit 10.10.101.0 0.0.0.255
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
access-list (IP standard)	Defines a standard IP access list.
distribute-list in (IP)	Filters networks received in updates.
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.

interval (BFD)

To configure the transmit and receive intervals between BFD packets, and to specify the number of consecutive BFD control packets that must be missed before BFD declares that a peer is unavailable, use the **interval** command in BFD configuration mode. To disable interval values use the **no** form of this command.

interval {both *milliseconds* **| min-tx** *milliseconds* **min-rx** *milliseconds*} [**multiplier** *multiplier-value*]

no interval

Syntax Description

both *milliseconds*	Specifies the rate at which BFD control packets are sent to BFD peers and the rate at which BFD control packets are received from BFD peers. Range is from 50 to 999 milliseconds (ms).
min-tx *milliseconds*	Specifies the rate at which BFD control packets are sent to BFD peers. Range is from 50 to 999 ms.
min-rx *milliseconds*	Specifies the rate at which BFD control packets are received from BFD peers. Range is from 50 to 999 ms.
multiplier *multiplier-value*	(Optional) Specifies the number of consecutive BFD control packets that must be missed from a BFD peer before BFD declares that the peer is unavailable and the Layer 3 BFD peer is informed of the failure. Range is from 3 to 50. Default is 3.

Command Default

No session parameters are set.

Command Modes

BFD configuration (config-bfd)

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

Command	Description
bfd	Set the baseline BFD session parameters on an interface.
bfd all-interfaces	Enables BFD for all interfaces participating in the routing process.

Command	Description
bfd echo	Enables BFD echo mode.
bfd interface	Enables BFD on a per-interface basis for a BFD peer.
bfd slow-timer	Configures the BFD slow timer value.
bfd-template	Creates a BFD template and enters BFD configuration mode.

ip default-network

To select a network as a candidate route for computing the gateway of last resort, use the **ip default-network** command in global configuration mode. To remove a route, use the **no** form of this command.

ip default-network *network-number*

no ip default-network *network-number*

Syntax Description

network-number	Number of the network.

Command Default

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

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

Examples

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

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

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

```
ip default-network 10.140.0.0
```

Related Commands

Command	Description
show ip route	Displays the current state of the routing table.

ip gdp

To configure the router discovery mechanism, use the **ip gdp** command in global configuration mode. To disable the configuration, use the **no** form of this command.

ip gdp {**eigrp** | **irdp** [**multicast**] | **rip**}

no ip gdp {**eigrp** | **irdp** [**multicast**] | **rip**}

Syntax Description

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

Command Default

The router discovery mechanism is not configured.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

You must disable IP routing to configure the **ip gdp** command.

Examples

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

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

Related Commands

Command	Description
ip host	Defines static hostname-to-address mappings in the DNS hostname cache for a DNS view.
ip route	Establishes static routes.

ip local policy route-map

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

ip local policy route-map *map-tag*

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

Syntax Description

map-tag	Name of the route map to use for local policy routing. The name must match a *map-tag* value specified by a **route-map** command.

Defaults

Packets that are generated by the router are not policy routed.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

The **ip local policy route-map** command identifies a route map to use for local policy routing. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*—the conditions under which packets should be policy routed. The **set** commands specify the *set actions*—the particular policy routing actions to perform if the criteria enforced by the **match** commands are met. The **no ip local policy route-map** command deletes the reference to the route map and disables local policy routing.

Examples

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

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

Related Commands

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

ip policy route-map

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

ip policy route-map *map-tag*

no ip policy route-map

Syntax Description

map-tag	Name of the route map to use for policy routing. The name must match a *map-tag* value specified by a **route-map** command.

Defaults

No policy routing occurs on the interface.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

The **ip policy route-map** command identifies a route map to use for policy routing. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*—the conditions under which policy routing is allowed for the interface, based on the destination IP address of the packet. The **set** commands specify the *set actions*—the particular policy routing actions to perform if the criteria enforced by the **match** commands are met. The **no ip policy route-map** command deletes the pointer to the route map.

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

Examples

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

```
interface serial 0
 ip policy route-map policy_marketing
!
```

```
route-map policy_marketing
 match ip address 172.21.16.18
 set ip next-hop 172.30.3.20
```

Related Commands

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

ip route

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

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

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

Syntax Description

vrf *vrf-name*	(Optional) Configures the name of the VRF by which static routes should be specified.
prefix	IP route prefix for the destination.
mask	Prefix mask for the destination.
ip-address	IP address of the next hop that can be used to reach that network.
interface-type interface-number	Network interface type and interface number.
dhcp	(Optional) Enables a Dynamic Host Configuration Protocol (DHCP) server to assign a static route to a default gateway (option 3). **Note** Specify the **dhcp** keyword for each routing protocol.
distance	(Optional) Administrative distance. The default administrative distance for a static route is 1.
name *next-hop-name*	(Optional) Applies a name to the next hop route.
permanent	(Optional) Specifies that the route will not be removed, even if the interface shuts down.
track *number*	(Optional) Associates a track object with this route. Valid values for the *number* argument range from 1 to 500.
tag *tag*	(Optional) Tag value that can be used as a "match" value for controlling redistribution via route maps.

Command Default

No static routes are established.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.3(2)XE	The **track** keyword and *number* argument were added.
12.3(8)T	The **track** keyword and *number* argument were integrated into Cisco IOS Release 12.3(8)T. The **dhcp** keyword was added.

Release	Modification
12.3(9)	The changes made in Cisco IOS Release 12.3(8)T were added to Cisco IOS Release 12.3(9).
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

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

When you specify a DHCP server to assign a static route, the interface type and number and administrative distance may be configured also.

If you specify an administrative distance, you are flagging a static route that can be overridden by dynamic information. For example, routes derived with Enhanced Interior Gateway Routing Protocol (EIGRP) have a default administrative distance of 90. To have a static route that would be overridden by an EIGRP dynamic route, specify an administrative distance greater than 100. Static routes have a default administrative distance of 100.

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

```
rtr1 (serial 172.16.188.1/30)--------------> rtr2(Fast Ethernet 172.31.1.1/30) ------>

router [rip | eigrp]
 network 172.16.188.0
 network 172.31.0.0
```

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

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

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

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

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

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

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

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

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

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

Specifying a numerical next hop that is on a directly connected interface will prevent the router from using proxy ARP. However, if the interface with the next hop goes down and the numerical next hop can be reached through a recursive route, you may specify both the next hop and interface (for example, **ip route 0.0.0.0 0.0.0.0 ethernet 1/2 10.1.2.3**) with a static route to prevent routes from passing through an unintended interface.

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

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

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

Recursive Static Routing

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

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

```
ip route 192.168.1.1 255.255.255.255 10.0.0.2
```

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

The following example defines a valid recursive IPv4 static route:

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

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

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

It is not normally useful to manually configure a self-recursive static route, although it is not prohibited. However, a recursive static route that has been inserted in the IPv4 routing table may become self-recursive as a result of some transient change in the network learned through a dynamic routing protocol. If this situation occurs, the fact that the static route has become self-recursive will be detected and the static route will be removed from the IPv4 routing table, although not from the configuration. A subsequent network change may cause the static route to no longer be self-recursive, in which case it will be re-inserted in the IPv4 routing table.

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

Examples

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

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

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

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

```
ip route 172.31.0.0 255.255.0.0 172.31.6.6
```

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

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

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

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

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

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

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

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

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

```
Router# show running-config | include ip route

ip route 172.0.0.0 255.0.0.0 10.0.0.1 name Seattle2Detroit
```

Related Commands

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

ip route profile

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

ip route profile

no ip route profile

Syntax Description

This command has no arguments or keywords.

Defaults

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

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

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

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

Routing table statistics are collected for the following events:

- Forward-Path Change. This statistic is the number of changes in the forwarding path, which is the accumulation of prefix-add, next-hop change, and pathcount change statistics.
- Prefix-Add. A new prefix was added to the routing table.
- Next-Hop Change. A prefix is not added or removed, but the next hop changes. This statistic is only seen with recursive routes that are installed in the routing table.

- Pathcount Change. The number of paths in the routing table has changed. This statistic is the result of an increase in the number of paths for an Interior Gateway Protocol (IGP) prefix in the routing table.
- Prefix Refresh. Standard routing table maintenance; the forwarding behavior is not changed.

Use the **show ip route profile** command to display the routing table change statistics.

Examples

The following example enables the collection of routing table statistics:

```
ip route profile
```

Related Commands

Command	Description
show ip route profile	Displays routing table change statistics.

ip route static adjust-time

To change the time interval for IP static route adjustments during convergence, use the **ip route static adjust-time** command in global configuration mode. To reinstate the default adjustment time of 60 seconds, use the **no** form of this command.

ip route static adjust-time *seconds*

no ip route static adjust-time *seconds*

Syntax Description

seconds	Time of delay, in seconds, for convergence time during which the background process that monitors next-hop reachability is performed. The delay in convergence occurs when the route that covers the next hop is removed. The range is from 1 to 60. The default is 60.

Defaults

seconds: 60

Command Modes

Global configuration

Command History

Release	Modification
12.0(29)S	This command was introduced.
12.3(10)	This command was integrated into Cisco IOS Release 12.3(10).
12.3(11)T	This command was integrated into Cisco IOS Release 12.3(11)T.

Usage Guidelines

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

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

Examples

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

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

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

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

Related Commands

Command	Description
show ip route	Displays the current state of the routing table.

ip route static bfd

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

ip route static bfd *interface-type interface-number ip-address* [**group** *group-name* [**passive**]]

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

Syntax Description

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

Command Default

No static BFD neighbors are specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
15.1(2)S	This command was modified. The **group** *group-name* keyword-argument pair and the **passive** keyword were added.

Usage Guidelines

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

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

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

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

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

Examples

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

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

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

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

Related Commands

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

ip routing

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

ip routing

no ip routing

Syntax Description

This command has no arguments or keywords.

Defaults

IP routing is enabled.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

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

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

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

Examples

The following example enables IP routing:

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

ip routing protocol purge interface

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

ip routing protocol purge interface

no ip routing protocol purge interface

Syntax Description

This command has no arguments or keywords.

Command Default

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

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

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

If the **no ip routing protocol purge interface** command is executed and a link goes down, the RIB process is automatically triggered to delete all prefixes that have the next hop on this interface from the RIB. The protocols on all the routers are notified, and if there is a secondary path, the protocols will update the RIB with the new path. When the process works through a large routing table, the process can consume many CPU cycles and increase the convergence time.

Examples

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

```
Router# configure terminal

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

key

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

key *key-id*

no key *key-id*

Syntax Description

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

Command Default

No key exists on the key chain.

Command Modes

Key-chain configuration

Command History

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

Usage Guidelines

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

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

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

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

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

Examples

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

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

Related Commands

Command	Description
accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.
ipv6 authentication key-chain eigrp	Enables authentication of EIGRP packets for IPv6.
key chain	Enables authentication for routing protocols.
key-string (authentication)	Specifies the authentication string for a key.
send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.
show key chain	Displays authentication key information.

key chain

To enable authentication for routing protocols, identify a group of authentication keys by using the **key chain** command in global configuration mode. To remove the key chain, use the **no** form of this command.

key chain *name-of-chain*

no key chain *name-of-chain*

Syntax Description

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

Command Default

No key chain exists.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

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

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.

```
interface ethernet 0
 ip rip authentication key-chain chain1
 ip rip authentication mode md5
!
router rip
 network 172.19.0.0
```

```
 version 2
!
key chain chain1
 key 1
 key-string key1
 accept-lifetime 13:30:00 Jan 25 1996 duration 7200
 send-lifetime 14:00:00 Jan 25 1996 duration 3600
  key 2
  key-string key2
  accept-lifetime 14:30:00 Jan 25 1996 duration 7200
  send-lifetime 15:00:00 Jan 25 1996 duration 3600
```

Related Commands

Command	Description
accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.
ip rip authentication key-chain	Enables authentication for RIP Version 2 packets and specifies the set of keys that can be used on an interface.
ipv6 authentication key-chain eigrp	Enables authentication of EIGRP packets for IPv6.
key	Identifies an authentication key on a key chain.
key-string (authentication)	Specifies the authentication string for a key.
send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.
show key chain	Displays authentication key information.

key-string (authentication)

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

key-string *text*

no key-string *text*

Syntax Description

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

Command Default

No key exists.

Command Modes

Key chain key configuration

Command History

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

Usage Guidelines

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

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

Examples

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

```
interface ethernet 0
 ip rip authentication key-chain chain1
 ip rip authentication mode md5
!
router rip
 network 172.19.0.0
 version 2
```

```
!
key chain chain1
 key 1
 key-string key1
 accept-lifetime 13:30:00 Jan 25 1996 duration 7200
 send-lifetime 14:00:00 Jan 25 1996 duration 3600
 key 2
 key-string key2
 accept-lifetime 14:30:00 Jan 25 1996 duration 7200
 send-lifetime 15:00:00 Jan 25 1996 duration 3600
```

Related Commands

Command	Description
accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.
ipv6 authentication key-chain eigrp	Enables authentication of EIGRP packets for IPv6.
key	Identifies an authentication key on a key chain.
key chain	Enables authentication for routing protocols.
send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.
service password-encryption	Encrypts passwords.
show key chain	Displays authentication key information.

match interface (IP)

To distribute any routes that have their next hop out one of the interfaces specified, use the **match interface** command in route-map configuration mode. To remove the **match interface** entry, use the **no** form of this command.

match interface *interface-type interface-number* [*... interface-type interface-number*]

no match interface *interface-type interface-number* [*... interface-type interface-number*]

Syntax Description

interface-type	Interface type.
interface-number	Interface number.

Defaults

No match interfaces are defined.

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

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

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

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

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

Examples

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

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

Related Commands

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

match ip address

To distribute any routes that have a destination network number address that is permitted by a standard access list, an extended access list, or a prefix list, or to perform policy routing on packets, use the **match ip address** command in route-map configuration mode. To remove the **match ip address** entry, use the **no** form of this command.

match ip address {*access-list-number* [*access-list-number...* | *access-list-name...*] | *access-list-name* [*access-list-number...*| *access-list-name*] | **prefix-list** *prefix-list-name* [*prefix-list-name...*]}

no match ip address {*access-list-number* [*access-list-number...* | *access-list-name...*] | *access-list-name* [*access-list-number...*| *access-list-name*] | **prefix-list** *prefix-list-name* [*prefix-list-name...*]}

Syntax Description

access-list-number...	Number of a standard or extended access list. It can be an integer from 1 to 199. The ellipsis indicates that multiple values can be entered.
access-list-name...	Name of a standard or extended access list. It can be an integer from 1 to 199. The ellipsis indicates that multiple values can be entered.
prefix-list	Distributes routes based on a prefix list.
prefix-list-name...	Name of a specific prefix list. The ellipsis indicates that multiple values can be entered.

Defaults

No access list numbers or prefix lists are specified.

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

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

Like matches in the same route map subblock are filtered with “or” semantics. If any one match clause is matched in the entire route map subblock, this match is treated as a successful match. Dissimilar match clauses are filtered with “and” semantics. So dissimilar matches are filtered logically. If the first set of conditions is not met, the second match clause is filtered. This process continues until a match occurs or there are no more match clauses.

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

Redistribution

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

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

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

Policy Routing

Another purpose of route maps is to enable policy routing. The **match ip address** command allows you to policy route packets based on criteria that can be matched with an extended access list; for example, a protocol, protocol service, and source or destination IP address. To define the conditions for policy routing packets, use the **ip policy route-map** interface configuration command, in addition to the **route-map** global configuration command, and the **match** and **set** route-map configuration commands. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*—the conditions under which policy routing occurs. The **set** commands specify the *set actions*—the particular routing actions to perform if the criteria enforced by the **match** commands are met. You might want to policy route packets based on their source, for example, using an access list.

Examples

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

```
route-map name
 match ip address 5 80
```

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

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

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

```
interface serial 0
 ip policy route-map chicago
!
route-map chicago
 match ip address 6 25
 set interface ethernet 0
```

Related Commands

Command	Description
ip local policy route-map	Identifies a route map to use for policy routing on an interface.
ip policy route-map	Identifies a route map to use for policy routing on an interface.
match as-path	Matches a BGP autonomous system path access list.
match community	Matches a BGP community.
match interface (IP)	Distributes any routes that have their next hop out one of the interfaces specified.
match ip next-hop	Redistributes any routes that have a next hop router address passed by one of the access lists specified.
match ip redistribution-source	Filters the external EIGRP routes that have been advertised by routers and access servers at the address specified by the access lists.
match ip route-source	Matches routes that have been advertised by routers and access servers at the address specified by the access lists.
match length	Bases policy routing on the Level 3 length of a packet.
match metric (IP)	Redistributes routes with the metric specified.
match route-type (IP)	Redistributes routes of the specified type.
match tag	Redistributes routes in the routing table that match the specified tags.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set as-path	Modifies an autonomous system path for BGP routes.
set automatic-tag	Automatically computes the tag value.
set community	Sets the BGP communities attribute.
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Indicates where to output packets that pass a match clause of a route map for policy routing.
set ip default next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing and for which the Cisco IOS software has no explicit route to a destination.
set ip next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing.
set level (IP)	Indicates where to import routes.
set local-preference	Specifies a preference value for the autonomous system path.
set metric (BGP, OSPF, RIP)	Sets the metric value for a routing protocol.

Command	Description
set metric-type	Sets the metric type for the destination routing protocol.
set next-hop	Specifies the address of the next hop.
set tag (IP)	Sets a tag value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.

match ip next-hop

To redistribute any routes that have a next hop router address passed by one of the access lists specified, use the **match ip next-hop** command in route-map configuration mode. To remove the next hop entry, use the **no** form of this command.

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

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

Syntax Description

access-list-number | *access-list-name*	Number or name of a standard or extended access list. It can be an integer from 1 to 199.

Defaults

Routes are distributed freely, without being required to match a 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

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

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

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

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

Examples

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

```
route-map name
 match ip next-hop 5 80
```

Related Commands

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

match ip redistribution-source

To match the external Enhanced Interior Gateway Routing Protocol (EIGRP) routes that have been advertised by routers and access servers at the address specified by the access lists, use the **match ip redistribution-source** command in route-map configuration mode. To remove the redistribution-source entry, use the **no** form of this command.

match ip redistribution-source [*access-list-number* [*...access-list-number*]] [*expanded-access-list* [*...expanded-access-list*]] [*access-list-name* [*...access-list-name*]] [**prefix-list** *name* [*...***prefix-list** *name*]]

no match ip redistribution-source [*access-list-number* [*...access-list-number*]] [*expanded-access-list* [*...expanded-access-list*]] [*access-list-name* [*...access-list-name*]] [**prefix-list** *name* [*...***prefix-list** *name*]]

Syntax Description

access-list-number	(Optional) Number of a standard access list. The range is from 1 to 199.
expanded-access-list	(Optional) Number of an expanded access list. The range is from from 1300 to 1999.
access-list-name	(Optional) Name of a standard access list.
prefix-list *name*	(Optional) Specifies the match entries of a specified prefix list.

Command Default

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

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
15.1(3)T	This command was introduced in Cisco IOS Release 15.1(3)T.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S and implemented on Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

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

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

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

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

Examples

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

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

Related Commands

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

match ip route-source

To match routes that have been advertised by routers and access servers at the address specified by the access lists, use the **match ip route-source** command in route-map configuration mode. To remove the route-source entry, use the **no** form of this command.

match ip route-source [*access-list-number* [*...access-list-number*]] [*expanded-access-list* [*...expanded-access-list*]] [*access-list-name* [*...access-list-name*]] [**prefix-list** *name* [*...***prefix-list** *name*]] [**redistribution-source**]

no match ip route-source [*access-list-number* [*...access-list-number*]] [*expanded-access-list* [*...expanded-access-list*]] [*access-list-name* [*...access-list-name*]] [**prefix-list** *name* [*...***prefix-list** *name*]] [**redistribution-source**]

Syntax Description

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

Command Default

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

Command Modes

Route-map configuration (config-route-map)

Command History

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

Usage Guidelines

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

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

specify the match criteria—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

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

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

Examples

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

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

Related Commands

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

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

match length

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

match length *minimum-length maximum-length*

no match length *minimum-length maximum-length*

Syntax Description

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

Command Default

No policy routing occurs on the length of a packet.

Command Modes

Route-map configuration

Command History

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

Usage Guidelines

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

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

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

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

Examples

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

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

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

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

Related Commands

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

match metric (IP)

To redistribute routes with the specified metric, use the **match metric** command in route-map configuration mode. To remove the entry for the redistributed route from the routing table, use the **no** form of this command.

match metric {*metric-value* | **external** *metric-value*} [**+-** *deviation-number*]

no match metric {*metric-value* | **external** *metric-value*} [**+-** *deviation-number*]

Syntax Description

metric-value	Internal route metric, which can be an Enhanced Interior Gateway Routing Protocol (EIGRP) five-part metric. The range is from 1 to 4294967295.
external	External protocol associated with a route and interpreted by a source protocol.
+- *deviation-number*	(Optional) A standard deviation number that will offset the number configured for the *metric-value* argument. The *deviation-number* argument can be any number. There is no default. **Note** When you specify a deviation of the metric with the **+** and **-** keywords, the router will match any metric that falls inclusively in that range.

Command Default

No filtering is performed on a metric value.

Command Modes

Route-map configuration

Command History

Release	Modification
11.2	This command was introduced.
12.3(8)T	The **external** and **+-** keywords and *deviation-number* argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

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

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

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

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

Examples

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

```
route-map name
 match metric 5
```

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

```
route-map name
 match metric 500 +- 100
```

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

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

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community	Matches a BGP community.
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 redistribution-source	Filters the external EIGRP routes that have been advertised by routers and access servers at the address specified by the access lists.
match ip route-source	Matches routes that have been advertised by routers and access servers at the address specified by the access lists.
match route-type (IP)	Redistributes routes of the specified type.
match tag	Redistributes routes in the routing table that match the specified tags.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.

Command	Description
set as-path	Modifies an autonomous system path for BGP routes.
set automatic-tag	Automatically computes the tag value.
set community	Sets the BGP communities attribute.
set level (IP)	Indicates where to import routes.
set local-preference	Specifies a preference value for the autonomous system path.
set metric (BGP, OSPF, RIP)	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set next-hop	Specifies the address of the next hop.
set tag (IP)	Sets a tag value of the destination routing protocol.

match route-type (IP)

To redistribute routes of the specified type, use the **match route-type** command in route-map configuration mode. To remove the route type entry, use the **no** form of this command.

match route-type {**local** | **internal** | **external** [**type-1** | **type-2**] | **level-1** | **level-2**}

no match route-type {**local** | **internal** | **external** [**type-1** | **type-2**] | **level-1** | **level-2**}

Syntax Description

local	Locally generated Border Gateway Protocol (BGP) routes.
internal	Open Shortest Path First (OSPF) intra-area and interarea routes or Enhanced Interior Gateway Routing Protocol (EIGRP) internal routes.
external [**type-1** | **type-2**]	OSPF external routes, or EIGRP external routes. For OSPF, the **external type-1** keyword matches only Type 1 external routes and the **external type-2** keyword matches only Type 2 external routes.
level-1	Intermediate System-to-Intermediate System (IS-IS) Level 1 routes.
level-2	IS-IS Level 2 routes.

Defaults

This command is disabled by default.

Command Modes

Route-map configuration

Command History

Release	Modification
10.0	This command was introduced.
11.2	The **local** and **external** [**type-1** | **type-2**] keywords were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

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

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

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

Examples

The following example redistributes internal routes:

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

Related Commands

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

match tag

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

match tag *tag-value* [*...tag-value*]

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

Syntax Description

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

Command Default

No match tag values are defined.

Command Modes

Route-map configuration (config-route-map)

Command History

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

Usage Guidelines

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

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

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

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

Examples

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

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

Related Commands

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

maximum-paths

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

maximum-paths *number-paths*

no maximum-paths

Syntax Description

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

Command Default

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

Command Modes

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

Command History

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

Usage Guidelines

Release 12.2(33)SRB

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

Examples

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

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

nsf

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

nsf [**enforce global**]

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

no nsf

Syntax Description

enforce global	(Optional) Cancels OSPF NSF restart when non-NSF-aware neighbors are detected.
cisco	Specifies the Cisco proprietary IS-IS NSF method of checkpointing if the active RP fails over.
ietf	Specifies the IETF IS-IS NSF method of protocol modification if the active RP fails over.
interface wait *seconds*	(Optional) Specifies how long to wait for an interface to come up after failover before it proceeds with the Cisco NSF process; valid values are from 1 to 60 seconds.
interval *minutes*	(Optional) Specifies how long to wait after a route processor stabilizes before restarting; valid values are from 0 to 1440 minutes.
t3 adjacency	(Optional) Specifies that the time that IETF NSF waits for the LSP database to synchronize is determined by the adjacency holdtime advertised to the neighbors of the specified RP before switchover.
t3 manual *seconds*	(Optional) Specifies the time to wait after the NSF database synchronizes before informing other nodes to remove the restarting node from consideration as a transit; valid values are from 5 to 3600 seconds.

Defaults

The default settings are as follows:

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

Command Modes

Router configuration

Command History

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

Usage Guidelines

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

The **nsf interface wait** command can be used if Cisco proprietary IS-IS NSF is configured or if the Internet Engineering Task Force (IETF) IS-IS NSF is enabled using the **nsf t3** manual command. You can use this command if an interface is slow to come up.

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

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

- **nsf** under the **router ospf** command
- **nsf ietf** under the **router isis** command
- **bgp graceful-restart** under the **router bgp** command

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

The [{**cisco** | **ietf**} | **interface wait** *seconds* | **interval** *minutes* | **t3** [**adjacency** | **manual** *seconds*] keywords and arguments apply to IS-IS only.

The {**enforce global**} keywords apply to OSPF only.

BGP NSF Guidelines

BGP support in NSF requires that neighbor networking devices be NSF-aware devices; that is, they must have the graceful restart capability and advertise that capability in the OPEN message during session establishment. If an NSF-capable router discovers that a particular BGP neighbor does not have the graceful restart capability enabled, it will not establish an NSF-capable session with that neighbor. All other neighbors that have a graceful restart capability will continue to have NSF-capable sessions with this NSF-capable networking device. Enter the **bgp graceful-restart** router configuration command to enable the graceful restart capability.

EIRGP NSF Guidelines

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

IS-IS NSF Guidelines

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

Use these two keywords when configuring IS-IS NSF:

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

OSPF NSF Guidelines

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

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

Examples

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

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

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

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

Related Commands

Command	Description
router	Enables a routing process.

passive-interface

To disable sending routing updates on an interface, use the **passive-interface** command in router configuration mode. To re-enable the sending of routing updates, use the **no** form of this command.

passive-interface [**default**] i*nterface-type interface-number*

no passive-interface *interface-type interface-number*

Syntax Description

default	(Optional) Causes all interfaces to become passive.
interface-type	Interface type.
interface-number	Interface number.

Defaults

Routing updates are sent on the interface.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
10.0	This command was introduced.
12.0	This command was modified. The **default** keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

If you disable the sending of routing updates on an interface, the particular subnet will continue to be advertised to other interfaces, and updates from other routers on that interface continue to be received and processed.

The **default** keyword sets all interfaces as passive by default. You can then configure individual interfaces where adjacencies are desired using the **no passive-interface** command. The **default** keyword is useful in Internet service provider (ISP) and large enterprise networks where many of the distribution routers have more than 200 interfaces.

For the Open Shortest Path First (OSPF) protocol, OSPF routing information is neither sent nor received through the specified router interface. The specified interface address appears as a stub network in the OSPF domain.

For the Intermediate System-to-Intermediate System (IS-IS) protocol, this command instructs IS-IS to advertise the IP addresses for the specified interface without actually running IS-IS on that interface. The **no** form of this command for IS-IS disables advertising IP addresses for the specified address.

Note For IS-IS you must keep at least one active interface and configure the interface with the **ip router isis** command.

The use of the **passive-interface** command in Enhanced Interior Gateway Routing Protocol (EIGRP) suppresses the exchange of hello packets on the interface and thus stops routing updates from being advertised, and it also suppresses incoming routing updates. For more information on passive interfaces, see http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080093f0a.shtml.

Examples

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

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

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

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

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

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

platform bfd enable-offload

To enable a Bidirectional Forwarding Detection (BFD) session offload on a system, use the **platform bfd enable-offload** command in the global configuration mode. To disable the BFD session offload use the **no** form of this command.

platform bfd enable-offload

no platform bfd enable-offload

Syntax Description

This command has no arguments or keywords

Command Default

Command is disabled.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

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

Examples

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

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

redistribute (IP)

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

redistribute *protocol* [*process-id*] {**level-1** | **level-1-2** | **level-2**} [*autonomous-system-number*] [**metric** {*metric-value* | **transparent**}] [**metric-type** *type-value*] [**match** {**internal** | **external 1** | **external 2**}] [**tag** *tag-value*] [**route-map** *map-tag*] [**subnets**] [**nssa-only**]

no redistribute *protocol* [*process-id*] {**level-1** | **level-1-2** | **level-2**} [*autonomous-system-number*] [**metric** {*metric-value* | **transparent**}] [**metric-type** *type-value*] [**match** {**internal** | **external 1** | **external 2**}] [**tag** *tag-value*] [**route-map** *map-tag*] [**subnets**] [**nssa-only**]

Syntax Description

protocol	Source protocol from which routes are being redistributed. It can be one of the following keywords: **bgp**, **connected**, **eigrp**, **isis**, **mobile**, **ospf**, **static** [**ip**], or **rip**. The **static** [**ip**] keyword is used to redistribute IP static routes. The optional **ip** keyword is used when redistributing into the Intermediate System-to-Intermediate System (IS-IS) protocol. The **connected** keyword refers to routes that are established automatically by virtue of having enabled IP on an interface. For routing protocols such as Open Shortest Path First (OSPF) and IS-IS, these routes will be redistributed as external to the autonomous system.
process-id	(Optional) For the **bgp** or **eigrp** keyword, this is an autonomous system number, which is a 16-bit decimal number. For the **isis** keyword, this is an optional *tag* value that defines a meaningful name for a routing process. You can specify only one IS-IS process per router. Creating a name for a routing process means that you use names when configuring routing. For the **ospf** keyword, this is an appropriate OSPF process ID from which routes are to be redistributed. This identifies the routing process. This value takes the form of a nonzero decimal number. For the **rip** keyword, no *process-id* value is needed. By default, no process ID is defined.
level-1	Specifies that, for IS-IS, Level 1 routes are redistributed into other IP routing protocols independently.
level-1-2	Specifies that, for IS-IS, both Level 1 and Level 2 routes are redistributed into other IP routing protocols.
level-2	Specifies that, for IS-IS, Level 2 routes are redistributed into other IP routing protocols independently.

autonomous-system-number	(Optional) Autonomous system number for the redistributed route. Number in the range from 1 to 65535. • In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, 4-byte autonomous system numbers are supported in the range from 65536 to 4294967295 in asplain notation and in the range from 1.0 to 65535.65535 in asdot notation. • In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, 4-byte autonomous system numbers are supported in the range from 1.0 to 65535.65535 in asdot notation only. For more details about autonomous system number formats, see the **router bgp** command.
metric *metric-value*	(Optional) When redistributing from one OSPF process to another OSPF process on the same router, the metric will be carried through from one process to the other if no metric value is specified. When redistributing other processes to an OSPF process, the default metric is 20 when no metric value is specified. The default value is 0.
metric transparent	(Optional) Causes RIP to use the routing table metric for redistributed routes as the RIP metric.
metric-type *type-value*	(Optional) For OSPF, specifies the external link type associated with the default route advertised into the OSPF routing domain. It can be one of two values: • **1**—Type 1 external route • **2**—Type 2 external route If a **metric-type** is not specified, the Cisco IOS software adopts a Type 2 external route. For IS-IS, it can be one of two values: • **internal**—IS-IS metric that is < 63. • **external**—IS-IS metric that is > 64 < 128. The default is **internal**.
match {**internal** | **external 1** | **external 2**}	(Optional) For the criteria by which OSPF routes are redistributed into other routing domains. It can be one of the following: • **internal**—Routes that are internal to a specific autonomous system. • **external 1**—Routes that are external to the autonomous system, but are imported into OSPF as Type 1 external route. • **external 2**—Routes that are external to the autonomous system, but are imported into OSPF as Type 2 external route. The default is internal and external 1.

tag *tag-value*	(Optional) Specifies the 32-bit decimal value attached to each external route. This is not used by OSPF itself. It may be used to communicate information between Autonomous System Boundary Routers (ASBRs). If none is specified, then the remote autonomous system number is used for routes from Border Gateway Protocol (BGP) and Exterior Gateway Protocol (EGP); for other protocols, zero (0) is used.
route-map	(Optional) Specifies the route map that should be interrogated to filter the importation of routes from this source routing protocol to the current routing protocol. If not specified, all routes are redistributed. If this keyword is specified, but no route map tags are listed, no routes will be imported.
map-tag	(Optional) Identifier of a configured route map.
subnets	(Optional) For redistributing routes into OSPF, the scope of redistribution for the specified protocol. By default, no subnets are defined.
nssa-only	(Optional) Sets the nssa-only attribute for all routes redistributed into OSPF.

Command Default

Route redistribution is disabled.

Command Modes

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

Command History

Release	Modification
10.0	This command was introduced.
12.0(5)T	This command was modified. Address family configuration mode was added.
12.0(22)S	This command was modified. Address family support under EIGRP was added.
12.2(15)T	This command was modified. Address family support under EIGRP was added.
12.2(18)S	This command was modified. Address family support under EIGRP was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was modified. This command was made available in router address family topology configuration mode.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX.
12.0(32)S12	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.

Release	Modification
12.4(24)T	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.3	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SXI1	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is asplain.
Cisco IOS Release 15.0(1)M	This command was modified. The **nssa-only** keyword was added.
12.2(33)SRE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.

Usage Guidelines

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

A router receiving a link-state protocol with an internal metric will consider the cost of the route from itself to the redistributing router plus the advertised cost to reach the destination. An external metric only considers the advertised metric to reach the destination.

Routes learned from IP routing protocols can be redistributed at Level 1 into an attached area or at Level 2. The **level-1-2** keyword allows both Level 1 and Level 2 routes in a single command.

Redistributed routing information must be filtered by the **distribute-list out** router configuration command. This guideline ensures that only those routes intended by the administrator are passed along to the receiving routing protocol.

Whenever you use the **redistribute** or the **default-information** router configuration commands to redistribute routes into an OSPF routing domain, the router automatically becomes an ASBR. However, an ASBR does not, by default, generate a *default route* into the OSPF routing domain.

When routes are redistributed into OSPF from protocols other than OSPF or BGP, and no metric has been specified with the **metric-type** keyword and *type-value* argument, OSPF will use 20 as the default metric. When routes are redistributed into OSPF from BGP, OSPF will use 1 as the default metric. When routes are redistributed from one OSPF process to another OSPF process, Autonomous system (AS) external and not-so-stubby-area (NSSA) routes will use 20 as the default metric. When intra-area and inter-area routes are redistributed between OSPF processes, the internal OSPF metric from the redistribution source process is advertised as the external metric in the redistribution destination process. (This is the only case in which the routing table metric will be preserved when routes are redistributed into OSPF.)

When routes are redistributed into OSPF, only routes that are not subnetted are redistributed if the **subnets** keyword is not specified.

On a router internal to an NSSA area, the **nssa-only** keyword causes the originated type-7 NSSA LSAs to have their propagate (P) bit set to zero, which prevents area border routers from translating these LSAs into type-5 external LSAs. On an area border router that is connected to a NSSA and normal areas, the **nssa-only** keyword causes the routes to be redistributed only into the NSSA areas.

Routes configured with the **connected** keyword affected by this **redistribute** command are the routes not specified by the **network** router configuration command.

You cannot use the **default-metric** command to affect the metric used to advertise connected routes.

Note The **metric** value specified in the **redistribute** command supersedes the **metric** value specified using the **default-metric** command.

Default redistribution of IGPs or EGP into BGP is not allowed unless the **default-information originate** router configuration command is specified.

Using the no Form of the redistribute Command

Removing options that you have configured for the **redistribute** command requires careful use of the **no** form of the **redistribute** command to ensure that you obtain the result that you are expecting. See the "Examples" section for more information.

Release 12.2(33)SRB

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

4-Byte Autonomous System Number Support

In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, the Cisco implementation of 4-byte autonomous system numbers uses asplain—65538 for example—as the default regular expression match and output display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain format and the asdot format as described in RFC 5396. To change the default regular expression match and output display of 4-byte autonomous system numbers to asdot format, use the **bgp asnotation dot** command.

In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, the Cisco implementation of 4-byte autonomous system numbers uses asdot—1.2, for example—as the only configuration format, regular expression match, and output display, with no asplain support.

Examples

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

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

The following example causes EIGRP routes to be redistributed into an OSPF domain:

```
Router(config)# router ospf 110
Router(config-router)# redistribute eigrp
```

The following example causes the specified EIGRP process routes to be redistributed into an OSPF domain. The EIGRP-derived metric will be remapped to 100 and RIP routes to 200.

```
Router(config)# router ospf 109
Router(config-router)# redistribute eigrp 108 metric 100 subnets
Router(config-router)# redistribute rip metric 200 subnets
```

The following example configures BGP routes to be redistributed into IS-IS. The link-state cost is specified as 5, and the metric type will be set to external, indicating that it has lower priority than internal metrics.

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

In the following example, network 172.16.0.0 will appear as an external link-state advertisement (LSA) in OSPF 1 with a cost of 100 (the cost is preserved):

```
Router(config)# interface ethernet 0
Router(config-if)# ip address 172.16.0.1 255.0.0.0
Router(config)# ip ospf cost 100
Router(config)# interface ethernet 1
Router(config-if)# ip address 10.0.0.1 255.0.0.0
!
Router(config)# router ospf 1
Router(config-router)# network 10.0.0.0 0.255.255.255 area 0
Router(config-router)# redistribute ospf 2 subnet
Router(config)# router ospf 2
Router(config-router)# network 172.16.0.0 0.255.255.255 area 0
```

The following example shows how BGP routes are redistributed into OSPF and assigned the local 4-byte autonomous system number in asplain format. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, or a later release.

```
Router(config)# router ospf 2
Router(config-router)# redistribute bgp 65538
```

The following example removes the **connected metric 1000 subnets** options from the **redistribute connected metric 1000 subnets** command and leaves the **redistribute connected** command in the configuration:

```
Router(config-router)# no redistribute connected metric 1000 subnets
```

The following example removes the **metric 1000** options from the **redistribute connected metric 1000 subnets** command and leaves the **redistribute connected subnets** command in the configuration:

```
Router(config-router)# no redistribute connected metric 1000
```

The following example removes the **subnets** options from the **redistribute connected metric 1000 subnets** command and leaves the **redistribute connected metric 1000** command in the configuration:

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

The following example removes the **redistribute connected** command, and any of the options that were configured for the **redistribute connected** command, from the configuration:

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

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

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 1
Router(config-router-af)# topology base
Router(config-router-af-topology)# redistribute eigrp 6473 metric 1 1 1 1 1
```

Related Commands

Command	Description
address-family (EIGRP)	Enters address-family configuration mode to configure an EIGRP routing instance.
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.

Command	Description
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
bgp asnotation dot	Changes the default display and the regular expression match format of BGP 4-byte autonomous system numbers from asplain (decimal values) to dot notation.
default-information originate (BGP)	Allows the redistribution of network 0.0.0.0 into BGP.
default-information originate (IS-IS)	Generates a default route into an IS-IS routing domain.
default-information originate (OSPF)	Generates a default route into an OSPF routing domain.
distribute-list out (IP)	Suppresses networks from being advertised in updates.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
router bgp	Configures the BGP routing process.
router eigrp	Configures the EIGRP address-family process.
show route-map	Displays all route maps configured or only the one specified.
topology (EIGRP)	Configures an EIGRP process to route IP traffic under the specified topology instance and enters address family topology configuration mode.

route-map

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

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

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

Syntax Description

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

Command Default

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

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

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

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

Redistribution

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

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

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

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

Policy Routing

Another purpose of route maps is to enable policy routing. Use the **ip policy route-map** or **ipv6 policy route-map** command, in addition to the **route-map** command, and the **match** and **set** commands to define the conditions for policy routing packets. The **match** commands specify the conditions under which policy routing occurs. The **set** commands specify the routing actions to perform if the criteria enforced by the **match** commands are met. You might want to policy route packets some way other than the obvious shortest path.

The *sequence-number* argument works as follows:

1. If no entry is defined with the supplied tag, an entry is created with the *sequence-number* argument set to 10.
2. If only one entry is defined with the supplied tag, that entry becomes the default entry for the following **route-map** command. The *sequence-number* argument of this entry is unchanged.
3. If more than one entry is defined with the supplied tag, an error message is printed to indicate that the *sequence-number* argument is required.

If the **no route-map** *map-tag* command is specified (with no *sequence-number* argument), the whole route map is deleted.

Examples

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

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

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

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

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

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

Related Commands

Command	Description
ip policy route-map	Identifies a route map to use for policy routing on an interface.
ipv6 policy route-map	Configures IPv6 PBR on an interface.
match as-path	Matches a BGP autonomous system path access list.
match community	Matches a BGP community.
match interface (IP)	Distributes any routes that have their next hop out one of the interfaces specified.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.

Command	Description
match ipv6 address	Distributes IPv6 routes that have a prefix permitted by a prefix list or to specify an IPv6 access list to use to match packets for PBR for IPv6.
match ip next-hop	Redistributes any routes that have a next hop router address passed by one of the access lists specified.
match ip redistribution-source	Filters the external EIGRP routes that have been advertised by routers and access servers at the address specified by the access lists.
match ip route-source	Matches routes that have been advertised by routers and access servers at the address specified by the access lists.
match length	Bases policy routing on the Level 3 length of a packet.
match metric (IP)	Redistributes routes with the metric specified.
match route-type (IP)	Redistributes routes of the specified type.
match tag	Redistributes routes in the routing table that match the specified tags.
router eigrp	Configures the EIGRP address-family process.
set as-path	Modifies an autonomous system path for BGP routes.
set automatic-tag	Automatically computes the tag value.
set community	Sets the BGP communities attribute.
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Indicates where to output packets that pass a match clause of a route map for policy routing.
set ipv6 default next-hop	Specifies an IPv6 default next hop to which matching packets will be forwarded.
set ip default next-hop verify-availability	Indicates where to output packets that pass a match clause of a route map for policy routing and for which the Cisco IOS software has no explicit route to a destination.
set ip next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing.
set ipv6 next-hop (PBR)	Indicates where to output IPv6 packets that pass a match clause of a route map for PBR for IPv6.
set level (IP)	Indicates where to import routes.
set local preference	Specifies a preference value for the autonomous system path.
set metric (BGP, OSPF, RIP)	Sets the metric value for a routing protocol.
set metric type	Sets the metric type for the destination routing protocol.
set next-hop	Specifies the address of the next hop.
set tag (IP)	Sets a tag value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.

routing dynamic

To enable the router to pass routing updates to other routers through an interface, use the **routing dynamic** command in interface configuration mode. To disable the passing of routing updates through an interface, use the **no** form of this command.

routing dynamic

no routing dynamic

Syntax Description

This command has no arguments or keywords.

Command Default

Asynchronous interfaces: No routing updates are passed.
All other interface types: Routing updates are passed.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(11)T	This command was introduced. This command replaces the **async default routing** command.

Usage Guidelines

Use the **routing dynamic** command to control the passing of routing updates over an interface.

Issuing the **no routing dynamic** command flags the interface to indicate that routing updates should not be sent out of it.

The routing protocol must recognize the flag for this command to work as intended. The **routing dynamic** command sets and clears the flag; it does not enforce routing protocol conformance.

Examples

The following example enables routing over asynchronous interface 0:

```
interface async 0
 routing dynamic
```

The following example disables routing over serial interface 2/0:

```
interface serial 2/0
 no routing dynamic
```

Related Commands

Command	Description
async dynamic routing	Enables manually configured routing on an asynchronous interface.
passive-interface	Disables sending routing updates on an interface.