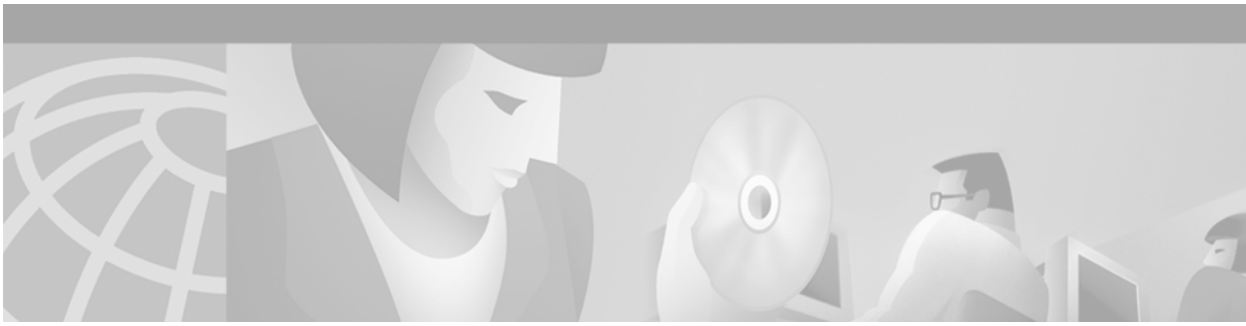

IP Routing Protocol-Independent Commands

Use the commands in this chapter to configure and monitor the features that are routing protocol-independent. For configuration information and examples on IP routing protocol-independent features, refer to the "Configuring IP Routing Protocol-Independent Features" chapter of the *Cisco IOS IP Configuration Guide*.

accept-lifetime

To set the time period during which the authentication key on a key chain is received as valid, use the **accept-lifetime** key chain key configuration command. 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.

Defaults

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

Command Modes

Key chain key configuration

Command History

Release	Modification
11.1	This command was introduced.

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 trees. The key named chestnut 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 birch 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 trees
 ip rip authentication mode md5
!
router rip
 network 172.19.0.0
 version 2
!
key chain trees
 key 1
 key-string chestnut
 accept-lifetime 13:30:00 Jan 25 1996 duration 7200
 send-lifetime 14:00:00 Jan 25 1996 duration 3600
 key 2
 key-string birch
 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.

distance (IP)

To define an administrative distance, use the **distance** command in router configuration mode. To remove a distance definition, use the **no** form of this command.

distance {*ip-address* {*wildcard-mask*}} [*ip-standard-list*] [*ip-extended-list*]

no distance {*ip-address* {*wildcard-mask*}} [*ip-standard-list*] [*ip-extended-list*]

Syntax Description

ip-address	IP address in four-part, dotted notation.
wildcard-mask	Wild card mask in four-part, dotted decimal format. A bit set to 1 in the *mask* argument instructs the software to ignore the corresponding bit in the address value.
ip-standard-list *ip-extended-list*	(Optional) Number or name of a standard or extended IP access list to be applied to incoming routing updates.

Defaults

For more information on default administrative distance, see "Usage Guidelines."

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
11.2	The *access-list-number* | *name* argument was added.
11.3	The *access-list-number* | *name* argument was removed.
11.3	The **ip** keyword was removed.
12.0	The *ip-standard-list* and *ip-extended-list* arguments were added.

Usage Guidelines

Table 51 lists default administrative distances.

Table 51 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
IGRP	100
Open Shortest Path First (OSPF)	110
Intermediate System-to-Intermediate System (IS-IS)	115

Table 51 Default Administrative Distances (continued)

Route Source	Default Distance
Routing Information Protocol (RIP)	120
Exterior Gateway Protocol (EGP)	140
EIGRP external route	170
Internal BGP	200
Unknown	255

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 that the routing information source cannot be trusted at all and should be ignored.

When the optional access list number 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 supplying the routing information. This option could be used, as an example, to filter out possibly incorrect routing information from routers 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** EXEC command displays the default administrative distance for a specified routing process.

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 igrp** global configuration command sets up IGRP routing in autonomous system number 109. The **network** router configuration commands specify IGRP routing on networks 192.168.7.0 and 172.16.0.0. The first **distance** router configuration command sets the default administrative distance to 255, which instructs the Cisco IOS software to ignore all routing updates from routers for which an explicit distance has not been set. The second **distance** command sets the administrative distance for all routers on the Class C network 192.168.7.0 to 90. The third **distance** command sets the administrative distance for the router with the address 172.16.1.3 to 120.

```
router igrp 109
 network 192.168.7.0
 network 172.16.0.0
 distance 255
 distance 90 192.168.7.0 0.0.0.255
 distance 120 172.16.1.3 0.0.0.0
```

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

```
router igrp 100
 network 10.0.0.0
 distance 22 10.0.0.0
 distance 33 10.11.0.0 0.0.255.255
 distance 44 10.11.12.0 0.0.0.255
```

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 is that the distance values are set to 255.

Related Commands

Command	Description
distance bgp	Allows the use of external, internal, and local administrative distances that could be a better route to a node.

distribute-list in (IP)

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

distribute-list {*access-list-number* | *access-list-name*} **in** [*interface-type interface-number*]

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

Syntax Description

access-list-number | *access-list-name*	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.
in	Applies the access list to incoming routing updates.
interface-type	(Optional) Interface type.
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.

Defaults

This command is disabled by default.

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
11.2	The *access-list-name*, *interface-type*, and *interface-number* arguments were added.

Usage Guidelines

This command is not supported in Intermediate System-to-Intermediate System (IS-IS) or Open Shortest Path First (OSPF). 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. We recommend this command not be used for OSPF.

Examples

In the following example, the EIGRP process accepts only 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
```

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 router 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.
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.

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
11.2	The *access-list-name* argument was added.

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.

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

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 and enables Intermediate System-to-Intermediate System (IS-IS) on Ethernet interface 0. Only network 10.10.101.0 will be advertised in outgoing IS-IS routing updates.

```
router isis
 redistribute ospf 109
 distribute-list 1 out
interface Ethernet 0
 ip router isis
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.

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.

Defaults

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; for Interior Gateway Routing Protocol (IGRP), it is the network itself, flagged as an exterior route.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

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 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.

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 172.130.3.20:

```
ip local policy route-map xyz
!
route-map xyz
 match ip address 131
 set ip next-hop 172.130.3.20
```

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

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.

Usage Guidelines

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

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

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

Examples

The following example sends packets with the destination IP address of 172.120.16.18 to a router at IP address 172.130.3.20:

```
interface serial 0
 ip policy route-map wethersfield
!
route-map wethersfield
 match ip address 172.120.16.18
 set ip next-hop 172.130.3.20
```

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 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.

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

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

Syntax Description

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) An administrative distance. The default administrative distance for a static route is 1.
name *next-hop-name*	(Optional) Associates a name with the next hop.
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.

Defaults

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.
12.3(9)	The changes made in Cisco IOS Release 12.3(8)T were added to Cisco IOS Release 12.3(9).

Release	Modification
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 100. To have a static route that would be overridden by an EIGRP dynamic route, specify an administrative distance greater than 100. Static routes have a default administrative distance of 1.

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

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

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

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

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

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

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

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

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

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

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

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.

The **name** *next-hop-name* keyword and argument combination allows you to identify 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.

Examples

The following example chooses 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 routes 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 routes 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 192.168.1.0 255.255.0.0 Ethernet 0 10.1.2.3
```

The following example installs 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 ether1 dhcp
ip route 10.165.200.226 255.255.255.255 ether2 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.

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 repeats.

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 routing protocol purge interface

To enable routing protocols to purge their routes when an interface goes down, use the **ip routing protocol purge interface** command in global configuration mode. To disable this function, 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

If this command is not executed and a link goes down, the less efficient Routing Information Base (RIB) process is automatically triggered to delete all prefixes from the RIB that have the next hop on this interface. When the process works through a large routing table, it can consume many CPU cycles and increase convergence time.

Command Modes

Global configuration

Command History

Release	Modification
12.0(25.03)S01	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(23.01)S	This command was integrated into Cisco IOS Release 12.2 (23.01)S.

Usage Guidelines

The **ip routing protocol purge interface** command enables routing protocols that are capable of responding to interface failures to delete dependent routes from the RIB when a link on a router goes down and the interface is removed from the routing table.

Examples

In the following example, the purge interface function is enabled for a routing protocol.

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip routing protocol purge interface
Router(config)# end
```

key

To identify an authentication key on a key chain, use the **key** key-chain configuration command. 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.

Defaults

No key exists on the key chain.

Command Modes

key-chain configuration

Command History

Release	Modification
11.1	This command was introduced.

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 trees. The key named chestnut 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 birch 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 trees
 ip rip authentication mode md5
!
router rip
 network 172.19.0.0
 version 2
!
key chain trees
 key 1
 key-string chestnut
 accept-lifetime 13:30:00 Jan 25 1996 duration 7200
 send-lifetime 14:00:00 Jan 25 1996 duration 3600
 key 2
 key-string birch
 accept-lifetime 14:30:00 Jan 25 1996 duration 7200
 send-lifetime 15:00:00 Jan 25 1996 duration 3600
```

Related Commands

Command	Description
accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.
key 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 2,147,483,647 keys.

Defaults

No key chain exists.

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.

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 trees. The key named chestnut 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 birch 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 trees
 ip rip authentication mode md5
!
router rip
 network 172.19.0.0
 version 2
!
key chain trees
 key 1
 key-string chestnut
 accept-lifetime 13:30:00 Jan 25 1996 duration 7200
 send-lifetime 14:00:00 Jan 25 1996 duration 3600
  key 2
  key-string birch
  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.
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** key chain key configuration command. 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.

Defaults

No key exists.

Command Modes

Key chain key configuration

Command History

Release	Modification
11.1	This command was introduced.

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 trees. The key named chestnut 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 birch 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 trees
 ip rip authentication mode md5
!
router rip
 network 172.19.0.0
 version 2
!
key chain trees
 key 1
 key-string chestnut
 accept-lifetime 13:30:00 Jan 25 1996 duration 7200
 send-lifetime 14:00:00 Jan 25 1996 duration 3600
 key 2
 key-string birch
 accept-lifetime 14:30:00 Jan 25 1996 duration 7200
 send-lifetime 15:00:00 Jan 25 1996 duration 3600
```

Related Commands

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

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-list	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 route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match metric (IP)	Redistributes routes with the metric specified.
match route-type (IP)	Redistributes routes of the specified type.
match tag	Redistributes routes in the routing table that match the specified tags.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set as-path	Modifies an autonomous system path for BGP routes.
set 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.

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 route-source	Redistributes 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.
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.

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-list	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 route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match metric (IP)	Redistributes routes with the metric specified.
match route-type (IP)	Redistributes routes of the specified type.
match tag	Redistributes routes in the routing table that match the specified tags.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set as-path	Modifies an autonomous system path for BGP routes.
set 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 route-source

To redistribute 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-name*}[*...access-list-number* | *...access-list-name*]

no match ip route-source {*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

No filtering on route source.

Command Modes

Route-map configuration

Command History

Release	Modification
10.0	This command was introduced.

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.

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.

There are situations in which the next hop and source router address of the route are not the same.

Examples

The following example distributes routes that have been advertised by routers and access servers at the addresses specified by access lists 5 and 80:

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

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community-list	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 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 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.

Defaults

No policy routing on the length of a packet.

Command Modes

Route-map configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

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.

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.

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
```

Related Commands

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

match metric (IP)

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

match metric *metric-value*

no match metric *metric-value*

Syntax Description

metric-value	Route metric, which can be an IGRP five-part metric. It is a metric value from 0 to 4294967295.

Defaults

No filtering on a metric value.

Command Modes

Route-map configuration

Command History

Release	Modification
11.2	This command was introduced.

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

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

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

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community-list	Matches a BGP community.
match interface (IP)	Distributes any routes that have their next hop out one of the interfaces specified.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match ip next-hop	Redistributes any routes that have a next hop router address passed by one of the access lists specified.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match 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 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.

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-list	Matches a BGP community.
match interface (IP)	Distributes any routes that have their next hop out one of the interfaces specified.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match ip next-hop	Redistributes any routes that have a next hop router address passed by one of the access lists specified.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match metric (IP)	Redistributes routes with the metric specified.
match 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.

Defaults

No match tag values are defined.

Command Modes

Route-map configuration

Command History

Release	Modification
10.0	This command was introduced.

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 second route map section with an explicit match specified.

Examples

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

```
route-map name
 match tag 5
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community-list	Matches a BGP community.
match interface (IP)	Distributes any routes that have their next hop out one of the interfaces specified.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match ip next-hop	Redistributes any routes that have a next hop router address passed by one of the access lists specified.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match metric (IP)	Redistributes routes with the metric specified.
match route-type (IP)	Redistributes routes of the specified type.
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 an IP routing protocol can support, use the **maximum-paths** command in router configuration mode. To restore the default value, use the **no** form of this command.

maximum-paths *number-paths*

no maximum-paths

Syntax Description

number-paths	Maximum number of parallel routes an IP routing protocol installs in a routing table, in the range from 1 to 6.

Defaults

The default for Border Gateway Protocol (BGP) is one path. The default for all other IP routing protocols is four paths.

Command Modes

Router configuration

Command History

Release	Modification
11.2	This command was introduced.

Examples

The following example allows a maximum of two paths to a destination:

```
maximum-paths 2
```

passive-interface

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

passive-interface [**default**] {*interface-type interface-number*}

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

Syntax Description

default	(Optional) All interfaces become passive.
interface-type	Interface type.
interface-number	Interface number.

Defaults

Routing updates are sent on the interface.

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0	The **default** keyword was added.

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.

Enhanced Interior Gateway Routing Protocol (EIGRP) is disabled on an interface that is configured as passive although it advertises the route.

Examples

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

```
router igrp 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, 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
```