

IP Routing Protocols Commands

Cisco's implementation of the Internet Protocol (IP) suite provides all major services contained in the TCP/IP specifications.

Use the commands in this chapter to configure and monitor the IP routing protocols. For IP routing protocol configuration information and examples, refer to the "Configuring IP Routing Protocols" chapter of the *Router Products Configuration Guide*.

aggregate-address

To create an aggregate entry in a BGP routing table, use the **aggregate-address** router configuration command. To disable this feature, use the **no** form of this command.

```
aggregate-address address mask [as-set] [summary-only] [suppress-map map-name]  
[advertise-map map-name] [attribute-map map-name]  
no aggregate-address address mask [as-set] [summary-only] [suppress-map map-name]  
[advertise-map map-name] [attribute-map map-name]
```

Syntax Description

<i>address</i>	Aggregate address.
<i>mask</i>	Aggregate mask.
as-set	(Optional) Generates autonomous system set path information.
summary-only	(Optional) Filters all more specific routes from updates.
suppress-map <i>map-name</i>	(Optional) Name of route map used to select the routes to be suppressed.
advertise-map <i>map-name</i>	(Optional) Name of route map used to select the routes to create AS-SET origin communities.
attribute-map <i>map-name</i>	(Optional) Name of route map used to set the attribute of the aggregate route.

Default

Disabled

Command Mode

Router configuration

Usage Guidelines

You can implement aggregate routing in BGP either by redistributing an aggregate route into BGP or by using this conditional aggregate routing feature.

Using the **aggregate-address** command with no arguments will create an aggregate entry in the BGP routing table if there are any more-specific BGP routes available that fall in the specified range. The aggregate route will be advertised as coming from your autonomous system and has the atomic aggregate attribute set to show that information might be missing. (By default, the atomic aggregate attribute is set unless you specify the **as-set** keyword.)

Using the **as-set** keyword creates an aggregate entry using the same rules that the command follows without this keyword, but the path advertised for this route will be an AS_SET consisting of all elements contained in all paths that are being summarized. Do not use this form of **aggregate-address** when aggregating many paths, because this route must be continually withdrawn and re-updated as autonomous system path reachability information for the summarized routes changes.

Using the **summary-only** keyword not only creates the aggregate route (for example, 193.*.*.*) but will also suppress advertisements of more specific routes to all neighbors. If you only want to suppress advertisements to certain neighbors, you may use the **neighbor distribute-list** command, with caution. If a more specific route leaks out, all BGP speakers will prefer that route over the less specific aggregate you are generating (using longest-match routing).

Using the **suppress-map** keyword creates the aggregate route but suppresses advertisement of specified routes. You can use the **match** clauses of route maps to selectively suppress some more specific routes of the aggregate and leave others unsuppressed. IP access lists and autonomous system path access lists match clauses are supported.

Example

In the following example, an aggregate address is created. The path advertised for this route will be an AS_SET consisting of all elements contained in all paths that are being summarized.

```
router bgp 5
aggregate-address 193.0.0.0 255.0.0.0 as-set
```

Related Commands

match as-path
match ip address
route-map

area authentication

To enable authentication for an OSPF area, use the **area authentication** router configuration command. To remove an area's authentication specification or a specified area from the router's configuration, use the **no** form of this command.

```
area area-id authentication [message-digest]
no area area-id authentication
no area area-id
```

Syntax Description

area-id	Identifier of the area for which authentication is to be enabled. The identifier can be specified as either a decimal value or an IP address.
message-digest	(Optional) Enables MD5 authentication on the area specified by <i>area-id</i> .

Default

Type 0 authentication (no authentication)

Command Mode

Router configuration

Usage Guidelines

Specifying authentication for an area sets the authentication to Type 1 (simple password) as specified in RFC 1247. If this command is not included in the configuration file, authentication of Type 0 (no authentication) is assumed.

The authentication type must be the same for all routers in an area. The authentication password for all OSPF routers on a network must be the same if they are to communicate with each other via OSPF. Use the **ip ospf authentication-key** command to specify this password.

If you enable MD5 authentication with the **message-digest** keyword, you must configure a password with the **ip ospf message-digest-key** command.

To remove the area's authentication specification, use the **no** form of this command with the **authentication** keyword. To remove the specified area from the router's configuration, use the command **no area area-id** (with no other keywords).

Example

The following example mandates authentication for areas 0 and 36.0.0.0 of OSPF routing process 201. Authentication keys are also provided.

```
interface ethernet 0
ip address 131.119.251.201 255.255.255.0
ip ospf authentication-key abcdefgh
!
interface ethernet 1
ip address 36.56.0.201 255.255.0.0
ip ospf authentication-key ijklnmop
!
```

```
router ospf 201
network 36.0.0.0 0.255.255.255 area 36.0.0.0
network 131.119.0.0 0.0.255.255 area 0
area 36.0.0.0 authentication
area 0 authentication
```

Related Commands

area default-cost
area stub
ip ospf authentication-key
ip ospf message-digest-key

area default-cost

To specify a cost for the default summary route sent into a stub area, use the **area default-cost** router configuration command. To remove the assigned default route cost, use the **no** form of this command.

```
area area-id default-cost cost
no area area-id default-cost cost
```

Syntax Description

<i>area-id</i>	Identifier for the stub area. The identifier can be specified as either a decimal value or as an IP address.
<i>cost</i>	Cost for the default summary route used for a stub area. The acceptable value is a 24-bit number.

Default

Cost of 1

Command Mode

Router configuration

Usage Guidelines

This command is used only on an area border router attached to a stub area.

There are two stub area router configuration commands: the **stub** and **default-cost** options of the **area** command. In all routers attached to the stub area, the area should be configured as a stub area using the **stub** option of the **area** command. Use the **default-cost** option only on an area border router attached to the stub area. The **default-cost** option provides the metric for the summary default route generated by the area border router into the stub area.

Example

The following example assigns a default-cost of 20 to stub network 36.0.0.0:

```
interface ethernet 0
ip address 36.56.0.201 255.255.0.0
!
router ospf 201
network 36.0.0.0 0.255.255.255 area 36.0.0.0
area 36.0.0.0 stub
area 36.0.0.0 default-cost 20
```

Related Commands

area authentication

area stub

area-password

To configure the IS-IS area authentication password, use the **area-password** router configuration command. To disable the password, use the **no** form of this command.

```
area-password password
no area-password [password]
```

Syntax Description

<i>password</i>	Password you assign.
-----------------	----------------------

Default

No area password is defined.

Command Mode

Router configuration

Usage Guidelines

This password is inserted in Level 1 (station router level) link state PDUs (LSPs), complete sequence number PDUs (CSNPs), and partial sequence number PDUs (PSNP).

Example

The following example assigns an area authentication password:

```
router isis
area-password angel
```

Related Command

domain-password

area range

To consolidate and summarize routes at an area boundary, use the **area range** router configuration command. To disable this function, use the **no** form of this command.

```
area area-id range address mask
no area area-id range address mask
```

Syntax Description

<i>area-id</i>	Identifier of the area about which routes are to be summarized. It can be specified as either a decimal value or as an IP address.
<i>address</i>	IP address.
<i>mask</i>	IP mask.

Default

Disabled

Command Mode

Router configuration

Usage Guidelines

The **area range** command is used only with area border routers. It is used to consolidate or summarize routes for an area. The result is that a single summary route is advertised to other areas by the area border router. Routing information is condensed at area boundaries. External to the area, a single route is advertised for each address range. This is called *route summarization*.

Multiple **area** router configuration commands specifying the **range** option can be configured. Thus, OSPF can summarize addresses for many different sets of address ranges.

Example

The following example specifies one summary route to be advertised by the area border router to other areas for all subnets on network 36.0.0.0 and for all hosts on network 192.42.110.0:

```
interface ethernet 0
ip address 192.42.110.201 255.255.255.0
!
interface ethernet 1
ip address 36.56.0.201 255.255.0.0
!
router ospf 201
network 36.0.0.0 0.255.255.255 area 36.0.0.0
network 192.42.110.0 0.0.0.255 area 0
area 36.0.0.0 range 36.0.0.0 255.0.0.0
area 0 range 192.42.110.0 255.255.255.0
```

area stub

To define an area as a stub area, use the **area stub** router configuration command. To disable this function, use the **no** form of this command.

```
area area-id stub [no-summary]
no area area-id stub
```

Syntax Description

area-id	Identifier for the stub area. The identifier can be either a decimal value or an IP address.
no-summary	(Optional) Prevents an Area Border Router from sending summary link advertisements into the stub area.

Default

No stub area is defined.

Command Mode

Router configuration

Usage Guidelines

You must configure the **area stub** command on all routers in the stub area. Use the **area** router configuration command with the **default-cost** option to specify the cost of a default internal router sent into a stub area by an area border router.

There are two stub area router configuration commands: the **stub** and **default-cost** options of the **area** router configuration command. In all routers attached to the stub area, the area should be configured as a stub area using the **stub** option of the **area** command. Use the **default-cost** option only on an area border router attached to the stub area. The **default-cost** option provides the metric for the summary default route generated by the area border router into the stub area.

To further reduce the number of link state advertisements (LSA) sent into a stub area, you can configure **no-summary** on the Area Border Router (ABR) to prevent it from sending summary link advertisement (LSA type 3) into the stub area.

Example

The following example assigns a default cost of 20 to stub network 36.0.0.0:

```
interface ethernet 0
ip address 36.56.0.201 255.255.0.0
!
router ospf 201
network 36.0.0.0 0.255.255.255 area 36.0.0.0
area 36.0.0.0 stub
area 36.0.0.0 default-cost 20
```

Related Commands

area authentication

area default-cost

area virtual-link

To define an OSPF virtual link, use the **area virtual-link** router configuration command with the optional parameters. To remove a virtual link, use the **no** form of this command.

```
area area-id virtual-link router-id [hello-interval seconds] [retransmit-interval seconds]
[transmit-delay seconds] [dead-interval seconds] [[authentication-key key] |
[message-digest-key keyid md5 key]]
no area area-id virtual-link router-id [hello-interval seconds] [retransmit-interval seconds]
[transmit-delay seconds] [dead-interval seconds] [[authentication-key key] |
[message-digest-key keyid md5 key]]
```

Syntax Description

<i>area-id</i>	Area ID assigned to the transit area for the virtual link. This can be either a decimal value or a valid IP address. There is no default.
<i>router-id</i>	Router ID associated with the virtual link neighbor. The router ID appears in the show ip ospf display. It is internally derived by each router from the router's interface IP addresses. This value must be entered in the format of an IP address. There is no default.
hello-interval <i>seconds</i>	(Optional) Time in seconds between the Hello packets that the router sends on an interface. Unsigned integer value to be advertised in the router's Hello packets. The value must be the same for all routers attached to a common network. The default is 10 seconds.
retransmit-interval <i>seconds</i>	(Optional) Time in seconds between link state advertisement retransmissions for adjacencies belonging to the interface. Expected round-trip delay between any two routers on the attached network. The value must be greater than the expected round-trip delay. The default is 5 seconds.
transmit-delay <i>seconds</i>	(Optional) Estimated time in seconds it takes to transmit a link state update packet on the interface. Integer value that must be greater than zero. Link state advertisements in the update packet have their age incremented by this amount before transmission. The default value is 1 second.
dead-interval <i>seconds</i>	(Optional) Time in seconds that a router's Hello packets are not seen before its neighbors declare the router down. Unsigned integer value. The default is four times the Hello interval, or 40 seconds. As with the Hello interval, this value must be the same for all routers attached to a common network.

authentication-key <i>key</i>	(Optional) Password to be used by neighboring routers. Any continuous string of characters that you can enter from the keyboard up to 8 bytes long. This string acts as a key that will allow the authentication procedure to generate or verify the authentication field in the OSPF header. This key is inserted directly into the OSPF header when originating routing protocol packets. A separate password can be assigned to each network on a per-interface basis. All neighboring routers on the same network must have the same password to be able to route OSPF traffic. The password is encrypted in the configuration file if the service password-encryption command is enabled. There is no default value.
message-digest-key <i>keyid md5 key</i>	(Optional) Key identifier and password to be used by neighboring routers and this router for MD5 authentication. The <i>keyid</i> is a number in the range 1 through 255. The <i>key</i> is an alphanumeric string of up to 16 characters. All neighboring routers on the same network must have the same key identifier and key to be able to route OSPF traffic. There is no default value.

Default

area-id: No area ID is predefined.

router-id: No router ID is predefined.

hello-interval *seconds*: 10 seconds

retransmit-interval *seconds*: 10 seconds

transmit-delay *seconds*: 1 second

dead-interval *seconds*: 40 seconds

authentication-key *key*: No key is predefined.

message-digest-key *keyid md5 key*: No key is predefined.

Command Mode

Router configuration

Usage Guidelines

In OSPF, all areas must be connected to a backbone area. If the connection to the backbone is lost, it can be repaired by establishing a virtual link.

The smaller the Hello interval, the faster topological changes will be detected, but more routing traffic will ensue.

The setting of the retransmit interval should be conservative, or needless retransmissions will result. The value should be larger for serial lines and virtual links.

The transmit delay value should take into account the transmission and propagation delays for the interface.

A router will use the specified authentication key only when authentication is enabled for the backbone with the **area** *area-id* **authentication** router configuration command.

The two authentication schemes, simple text and MD5 authentication, are mutually exclusive. You can specify one or the other or neither. Any keywords and arguments you specify after **authentication-key** *key* or **message-digest-key** *keyid* **md5** *key* are ignored. Therefore, specify any optional arguments before such a keyword-argument combination.

Note Each virtual link neighbor must include the transit area ID and the corresponding virtual link neighbor's router ID in order for a virtual link to be properly configured. Use the **show ip ospf** EXEC command to see the router ID of a router.

Examples

The following example establishes a virtual link with default values for all optional parameters:

```
router ospf 201
network 36.0.0.0 0.255.255.255 area 36.0.0.0
area 36.0.0.0 virtual-link 36.3.4.5
```

The following example establishes a virtual link with MD5 authentication:

```
router ospf 201
network 36.0.0.0 0.255.255.255 area 36.0.0.0
area 36.0.0.0 virtual-link 36.3.4.5 message-digest-key 3 md5 sa5721bk47
```

Related Commands

A dagger (†) indicates that the command is documented in another chapter.

area authentication
service password-encryption †
show ip ospf

autonomous-system (EGP)

To specify the local autonomous system that the router resides in for EGP, use the **autonomous-system** global configuration command. To remove the autonomous system number, use the **no** form of this command.

autonomous-system *local-as*
no autonomous-system *local-as*

Syntax Description

local-as Local autonomous system number to which the router belongs.

Default

No local autonomous system is specified.

Command Mode

Global configuration

Usage Guidelines

Before you can set up EGP routing, you must specify an autonomous system number. The local autonomous system number will be included in EGP messages sent by the router.

Example

The following sample configuration specifies an autonomous system number of 110:

```
autonomous-system 110
```

Related Command

router egp

auto-summary

To restore the default behavior of automatic summarization of subnet routes into network-level routes, use the **auto-summary** router configuration command. To disable this feature, use the **no** form of this command.

```
auto-summary
no auto-summary
```

Syntax Description

This command has no arguments or keywords.

Default

Enabled

Command Mode

Router configuration

Usage Guidelines

By default, BGP does not accept subnets redistributed from IGP. To advertise and carry subnet routes in BGP, use an explicit **network** command or the **no auto-summary** command. If you disable auto-summarization and have not entered a **network** command, you will not advertise network routes for networks with subnet routes unless they contain a summary route.

IP Enhanced IGRP summary routes are given an administrative distance value of 5. You cannot configure this value.

Examples

In the following example, network numbers are not summarized automatically:

```
router bgp 6
no auto-summary
```

The following example disables automatic summarization for router process eigrp 109:

```
router eigrp 109
no auto-summary
```

Related Command

ip summary-address eigrp

bgp always-compare-med

To allow the comparison of the Multi Exit Discriminator (MED) for paths from neighbors in different autonomous systems, use the **bgp always-compare-med** router configuration command. To disallow the comparison, use the **no** form of this command.

bgp always-compare-med
no bgp always-compare-med

Syntax Description

This command has no arguments or keywords.

Default

The router does not compare MEDs for paths from neighbors in different autonomous systems.

Command Mode

Router configuration

Usage Guidelines

The MED is one of the parameters that is considered when selecting the best path among many alternative paths. The path with a lower MED is preferred over a path with a higher MED.

By default, during the best path selection process, MED comparison is done only among paths from the same autonomous system. This command changes the default behavior by allowing comparison of MEDs among paths regardless of the autonomous system from which the paths are received.

Example

In the following example, the BGP speaker in autonomous system 100 is configured to compare MEDs among alternative paths, regardless of the autonomous system from which the paths are received:

```
router bgp 100
  bgp always-compare-med
```

bgp confederation identifier

To specify a BGP confederation identifier, use the **bgp confederation identifier** router configuration command. To remove the confederation identifier, use the **no** form of this command.

bgp confederation identifier *autonomous-system*
no bgp confederation identifier *autonomous-system*

Syntax Description

<i>autonomous-system</i>	Autonomous system number that internally includes multiple autonomous systems.
--------------------------	--

Default

No confederation identifier is configured.

Command Mode

Router configuration

Usage Guidelines

Another way to reduce the IBGP mesh is to divide an autonomous system into multiple autonomous systems and group them into a single confederation. Each autonomous system is fully meshed within itself, and has a few connections to another autonomous system in the same confederation. Even though the peers in different autonomous systems have EBGP sessions, they exchange routing information as if they are IBGP peers. Specifically, the next-hop and local preference information is preserved. This enables to you to retain a single Interior Gateway Protocol (IGP) for all of the autonomous systems. To the outside world, the confederation looks like a single autonomous system.

Example

In the following example, the autonomous system is divided into autonomous systems 4001, 4002, 4003, 4004, 4005, 4006, and 4007 and identified by the confederation identifier 5. Neighbor 1.2.3.4 is someone inside your routing domain confederation. Neighbor 3.4.5.6 is someone outside your routing domain confederation. To the outside world, there appears to be a single autonomous system with the number 5.

```
router bgp 4001
bgp confederation identifier 5
bgp confederation peers 4002 4003 4004 4005 4006 4007
neighbor 1.2.3.4 remote-as 4002
neighbor 3.4.5.6 remote-as 510
```

Related Command

bgp confederation peers

bgp confederation peers

To configure the autonomous systems that belong to the confederation, use the **bgp confederation peers** router configuration command. To remove an autonomous system from the confederation, use the **no** form of this command.

bgp confederation peers *autonomous-system* [*autonomous-system*]
no bgp confederation peers *autonomous-system* [*autonomous-system*]

Syntax Description

autonomous-system Autonomous system number.

Default

No confederation peers are configured.

Command Mode

Router configuration

Usage Guidelines

The autonomous systems specified in this command are visible internally to a confederation. Each autonomous system is fully meshed within itself. The **bgp confederation identifier** command specifies the confederation that the autonomous systems belong to.

Example

The following example specifies that autonomous systems 1090, 1091, 1092, and 1093 belong to a single confederation:

```
router bgp 1090
bgp confederation peers 1091 1092 1093
```

Related Command

bgp confederation identifier

bgp default local-preference

To change the default local preference value, use the **bgp default local-preference** router configuration command. To return to the default setting, use the **no** form of this command.

bgp default local-preference *value*
no bgp default local-preference *value*

Syntax Description

value Local preference value. Higher is more preferred. Integer from 0 through 4294967295.

Default

Local preference value of 100

Command Mode

Router configuration

Usage Guidelines

Generally, the default value of 100 allows you to easily define a particular path as less preferable than paths with no local preference attribute. The preference is sent to all routers in the local autonomous system.

Example

In the following example, the default local preference value is raised from the default of 100 to 200:

```
router bgp 200
  bgp default local-preference 200
```

Related Command

set local-preference

bgp fast-external-fallover

To immediately reset the BGP sessions of any directly adjacent external peers if the link used to reach them goes down, use the **bgp fast-external-fallover** router configuration command. To disable this feature, use the **no** form of this command.

```
bgp fast-external-fallover
no bgp fast-external-fallover
```

Syntax Description

This command has no arguments or keywords.

Default

Enabled

Command Mode

Router configuration

Example

In the following example, the automatic resetting of BGP sessions is disabled:

```
router bgp 109
no bgp fast-external-fallover
```

clear arp-cache

To remove all dynamic entries from the ARP cache and to clear the fast-switching cache, use the **clear arp-cache** EXEC command.

clear arp-cache

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

Example

The following example removes all dynamic entries from the ARP cache and clears the fast-switching cache:

clear arp-cache

clear ip bgp

To reset a BGP connection, use the **clear ip bgp** EXEC command at the system prompt.

clear ip bgp {* | address}

Syntax Description

*	Resets all current BGP sessions.
<i>address</i>	Resets only the identified BGP neighbor.

Command Mode

EXEC

Usage Guidelines

Use this command whenever any of the following changes occur:

- Additions or changes to the BGP-related access lists
- Changes to BGP-related weights
- Changes to BGP-related distribution lists
- Changes in the BGP timer's specifications
- Changes to the BGP administrative distance
- Changes to BGP-related route maps

Example

The following example resets all current BGP sessions:

```
clear ip bgp *
```

Related Commands

show ip bgp
timers bgp

clear ip bgp peer-group

To remove all of the members of a BGP peer group, use the **clear ip bgp peer-group** EXEC command.

clear ip bgp peer-group *tag*

Syntax Description

tag Name of the BGP peer group to clear.

Command Mode

EXEC

Example

The following example removes all members from the BGP peer group *internal*:

```
clear ip bgp peer-group internal
```

Related Command

neighbor peer-group (assigning members)

clear ip dvmrp route

To delete routes from the DVMRP routing table, use the **clear ip dvmrp route** EXEC command.

```
clear ip dvmrp route {* | route}
```

Syntax Description

<i>*</i>	Clears all routes.
<i>route</i>	Clears the longest matched route. Can be an IP address, a network number, or an IP DNS name.

Command Mode

EXEC

Examples

The following example deletes route 10.1.1.1 from the DVMRP routing table:

```
clear ip dvmrp route 10.1.1.1
```

The following example deletes network 10.0.0.0 from the DVMRP routing table:

```
clear ip dvmrp route 10.0.0.0
```

clear ip eigrp neighbors

To delete entries from the neighbor table, use the **clear ip eigrp neighbors** EXEC command.

clear ip eigrp neighbors [ip-address | type number]

Syntax Description

<i>ip-address</i>	(Optional) Address of the neighbor.
<i>type number</i>	(Optional) Interface type and number. Specifying these arguments removes from the neighbor table all entries learned via this interface.

Command Mode

EXEC

Example

The following example removes the neighbor whose address is 160.20.8.3:

```
clear ip eigrp neighbors 160.20.8.3
```

Related Command

show ip eigrp neighbors

clear ip igmp group

To delete entries from the IGMP cache, use the **clear ip igmp group** EXEC command.

clear ip igmp group [*group-name* | *group-address* | *type number*]

Syntax Description

<i>group-name</i>	(Optional) Name of the multicast group, as defined in the DNS hosts table or with the ip host command.
<i>group-address</i>	(Optional) Address of the multicast group. This is a multicast IP address in four-part dotted notation.
<i>type number</i>	(Optional) Interface type and number.

Command Mode

EXEC

Usage Guidelines

The IGMP cache contains a list of the multicast groups of which hosts on the directly connected LAN are members. If the router has joined a group, it is also listed in the cache.

To delete all entries from the IGMP cache, specify the **clear ip igmp group** command with no arguments.

Example

The following example clears entries for the multicast group 224.0.255.1 from the IGMP cache:

```
clear ip igmp group 224.0.255.1
```

Related Commands

A dagger (†) indicates that the command is documented in another chapter.

ip host †

show ip igmp groups

show ip igmp interface

clear ip mroute

To delete entries from the IP multicast routing table, use the **clear ip mroute** EXEC command.

clear ip mroute {* | group [source]}

Syntax Description

*	Deletes all entries from the IP multicast routing table.
<i>group</i>	Can be either one of the following: <ul style="list-style-type: none"> • Name of the multicast group, as defined in the DNS hosts table or with the ip host command. • IP address of the multicast group. This is a multicast IP address in four-part dotted notation.
<i>source</i>	(Optional) If you specify a group name or address, you can also specify a name or address of a multicast source that is transmitting to the group. A source does not need to be a member of the group.

Command Mode

EXEC

Examples

The following example deletes all entries from the IP multicast routing table:

```
clear ip mroute *
```

The following example deletes from the IP multicast routing table all sources on the 10.3.0.0 subnet that are transmitting to the multicast group 224.2.205.42. Note that this example deletes all sources on network 10.3, not individual sources.

```
clear ip mroute 224.2.205.42 10.3.0.0
```

Related Commands

A dagger (†) indicates that the command is documented in another chapter.

ip host †

show ip mroute

clear ip route

To remove one or more routes from the IP routing table, use the **clear ip route** EXEC command.

clear ip route {*network* [*mask*] | *}

Syntax Description

<i>network</i>	Network or subnet address to remove.
<i>mask</i>	(Optional) Network mask associated with the IP address you wish to remove.
*	Removes all entries.

Command Mode

EXEC

Example

The following example removes a route to network 132.5.0.0 from the IP routing table:

```
clear ip route 132.5.0.0
```

Related Command

show ip route

clear ip sd

To delete a session directory cache entry, use the **clear ip sd** EXEC command.

```
clear ip sd [group-address | "session-name"]
```

Syntax Description

group-address (Optional) All sessions associated with the IP group address are deleted.

"session-name" (Optional) Only the session directory entry by this name is deleted. The session name is enclosed in quotation marks and is not case-sensitive.

Command Mode

EXEC

Usage Guidelines

If neither argument is specified, the entire session directory cache is deleted.

Examples

The following example deletes the entire session directory cache:

```
clear ip sd
```

The following example deletes sessions with the group address 224.2.0.1 from the session directory cache:

```
clear ip sd 224.2.0.1
```

The following example deletes the session entry called *mbone audio* from the session directory cache:

```
clear ip sd "mbone audio"
```

Related Command

ip sd listen

default-information allowed

To control the candidate default routing information between IGRP or Enhanced IGRP processes, use the **default-information allowed** router configuration command. To suppress IGRP or Enhanced IGRP candidate information in incoming updates, use the **no default-information allowed in** command. To suppress IGRP or Enhanced IGRP candidate information in outbound updates, use the **no default-information allowed out** command.

```
default-information allowed {in | out} [route-map map-tag]
no default-information allowed {in | out} [route-map map-tag]
```

Syntax Description

in	Allows IGRP or Enhanced IGRP exterior or default routes to be received by an IGRP process.
out	Allows IGRP or Enhanced IGRP exterior routes to be advertised in updates.
route-map map-tag	(Optional) Indicates that the route map should be interrogated to filter the importation of routes from this source routing protocol to the current routing protocol. The argument <i>map-tag</i> is the identifier of a configured route map. If you specify route-map without specifying <i>map-tag</i> , no routes are imported. If you omit route-map , all routes are redistributed.

Default

Normally, exterior routes are always accepted and default information is passed between IGRP or Enhanced IGRP processes when doing redistribution.

Command Mode

Router configuration

Usage Guidelines

The default network of 0.0.0.0 used by RIP cannot be redistributed by IGRP or Enhanced IGRP.

Example

The following example allows IGRP exterior or default routes to be received by the IGRP process in autonomous system 23:

```
router igrp 23
default-information allowed in
```

default-information originate (BGP)

To allow the redistribution of network 0.0.0.0 into BGP, use the **default-information originate** router configuration command. To disable this feature, use the **no** form of this command.

```
default-information originate
no default-information originate
```

Syntax Description

This command has no arguments or keywords.

Default

Disabled

Command Mode

Router configuration

Usage Guidelines

The same functionality will result from the **network 0.0.0.0** command, using the **network** router configuration command.

Example

The following example configures BGP to redistribute network 0.0.0.0 into BGP:

```
router bgp 164
default-information originate
```

default-information originate (EGP)

To explicitly configure EGP to generate a default route, use the **default-information originate** router configuration command. To disable this feature, use the **no** form of this command.

```
default-information originate  
no default-information originate
```

Syntax Description

This command has no arguments or keywords.

Default

Disabled

Command Mode

Router configuration

Usage Guidelines

Because EGP can use network 0.0.0.0 as a default route, EGP must be explicitly configured to generate a default route. If the next hop for the default route can be advertised as a third party, it will be included as a third party.

Example

The following example configures EGP to generate a default route:

```
autonomous system 109
router ebgp 164
network 131.108.0.0
network 192.31.7.0
neighbor 10.2.0.2
default-information originate
```

default-information originate (IS-IS)

To generate a default route into an IS-IS routing domain, use the **default-information originate** router configuration command. To disable this feature, use the **no** form of this command.

```
default-information originate [route-map map-name]
no default-information originate [route-map map-name]
```

Syntax Description

route-map <i>map-name</i>	(Optional) Routing process will generate the default route if the route map is satisfied.
----------------------------------	---

Default

Disabled

Command Mode

Router configuration

Usage Guidelines

If a router configured with this command has a route to 0.0.0.0 in the routing table, IS-IS will originate an advertisement for 0.0.0.0 in its LSPs.

Example

In the following configuration, the router is forced to generate a default external route into an IS-IS domain:

```
router isis
  ! BGP routes will be distributed into IS-IS
  redistribute bgp 120
  ! access list 2 is applied to outgoing routing updates
  distribute-list 2 out
  default-information originate
  ! access list 2 defined as giving access to network 100.105.0.0
  access-list 2 permit 100.105.0.0 0.0.255.255
```

Related Commands

isis metric

redistribute

default-information originate (OSPF)

To generate a default route into an OSPF routing domain, use the **default-information originate** router configuration command. To disable this feature, use the **no** form of this command.

```
default-information originate [always] [metric metric-value] [metric-type type-value]
  {level-1 | level-1-2 | level-2} [route-map map-name]
no default-information originate [always] [metric metric-value] [metric-type type-value]
  {level-1 | level-1-2 | level-2} [route-map map-name]
```

Syntax Description

originate	Causes the router to generate a default external route into an OSPF domain if the router already has a default route and you want to propagate to other routers.
always	(Optional) Always advertises the default route regardless of whether the router has a default route.
metric <i>metric-value</i>	(Optional) Metric used for generating the default route. If you omit a value and do not specify a value using the default-metric router configuration command, the default metric value is 10. The value used is specific to the protocol.
metric-type <i>type-value</i>	(Optional) External link type associated with the default route advertised into the OSPF routing domain. It can be one of the following values: 1—Type 1 external route 2—Type 2 external route The default is Type 2 external route.
level-1	Level 1 routes are redistributed into other IP routing protocols independently. It specifies if IS-IS advertises network 0.0.0.0 into the Level 1 area.
level-1-2	Both Level 1 and Level 2 routes are redistributed into other IP routing protocols. It specifies if IS-IS advertises network 0.0.0.0 into both levels in a single command.
level-2	Level 2 routes are redistributed into other IP routing protocols independently. It specifies if IS-IS advertises network 0.0.0.0 into the Level 2 subdomain.
route-map <i>map-name</i>	(Optional) Routing process will generate the default route if the route-map is satisfied.

Default

Disabled

Command Mode

Router configuration

Usage Guidelines

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 autonomous system boundary router. However, an autonomous system boundary router does not, by default, generate a *default route* into the OSPF routing domain. The router still needs to have a default route for itself before it generates one, except when you have specified the **always** keyword.

When you use this command for the OSPF process, the default network must reside in the routing table and you must satisfy the **route-map map-name** keyword. Use the **default-information originate always route-map map-name** form of the command when you do not want the dependency on the default network in the routing table.

Example

The following example specifies a metric of 100 for the default route redistributed into the OSPF routing domain and an external metric type of Type 1:

```
router ospf 109
 redistribute igrp 108 metric 100 subnets
 default-information originate metric 100 metric-type 1
```

Related Command

redistribute

default-metric (BGP, EGP, OSPF, and RIP)

To set default metric values for the BGP, EGP, OSPF, and RIP routing protocols, use this form of the **default-metric** router configuration command. To return to the default state, use the **no** form of this command.

default-metric *number*
no default-metric *number*

Syntax Description

<i>number</i>	Default metric value appropriate for the specified routing protocol.
---------------	--

Default

Built-in, automatic metric translations, as appropriate for each routing protocol

Command Mode

Router configuration

Usage Guidelines

The **default-metric** command is used in conjunction with the **redistribute** router configuration command to cause the current routing protocol to use the same metric value for all redistributed routes. A default metric helps solve the problem of redistributing routes with incompatible metrics. Whenever metrics do not convert, using a default metric provides a reasonable substitute and enables the redistribution to proceed.

In BGP, this sets the multiple exit discriminator (MED) metric. (The name of this metric for BGP Versions 2 and 3 is **INTER_AS**.)

Example

The following example shows a router in autonomous system 109 using both the RIP and the OSPF routing protocols. The example advertises OSPF-derived routes using the RIP protocol and assigns the IGRP-derived routes a RIP metric of 10.

```
router rip
  default-metric 10
  redistribute ospf 109
```

Related Command

redistribute

default-metric (IGRP and Enhanced IGRP only)

To set metrics for IGRP or Enhanced IGRP, use this form of the **default-metric** router configuration command. To remove the metric value and restore the default state, use the **no** form of this command.

default-metric *bandwidth delay reliability loading mtu*
no default-metric *bandwidth delay reliability loading mtu*

Syntax Description

<i>bandwidth</i>	Minimum bandwidth of the route in kilobits per second. It can be 0 or any positive integer.
<i>delay</i>	Route delay in tens of microseconds. It can be 0 or any positive number that is a multiple of 39.1 nanoseconds.
<i>reliability</i>	Likelihood of successful packet transmission expressed as a number between 0 and 255. The value 255 means 100 percent reliability; 0 means no reliability.
<i>loading</i>	Effective bandwidth of the route expressed as a number from 0 to 255 (255 is 100 percent loading).
<i>mtu</i>	Minimum maximum transmission unit (MTU) size of the route in bytes. It can be 0 or any positive integer.

Default

Disabled

Command Mode

Router configuration

Usage Guidelines

Metric defaults have been carefully set to work for a wide variety of networks. Take great care in changing these values.

Keeping the same metrics is supported only when redistributing from IGRP, Enhanced IGRP, or static routes.

Example

The following example takes redistributed RIP metrics and translates them into IGRP metrics with values as follows: bandwidth = 1000, delay = 100, reliability = 250, loading = 100, and mtu = 1500.

```
router igrp 109
network 131.108.0.0
redistribute rip
default-metric 1000 100 250 100 1500
```

Related Command

redistribute

distance

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

```
distance weight [address mask [access-list-number]] [ip]  
no distance weight [address mask [access-list-number]] [ip]
```

Syntax Description

<i>weight</i>	Administrative distance. This can be an integer from 10 to 255. (The values 0 through 9 are reserved for internal use.) Used alone, the argument <i>weight</i> specifies a default administrative distance that the router uses when no other specification exists for a routing information source. Routes with a distance of 255 are not installed in the routing table.
<i>address</i>	(Optional) IP address in four-part dotted notation.
<i>mask</i>	(Optional) IP address mask in four-part dotted-decimal format. A bit set to 1 in the <i>mask</i> argument instructs the router to ignore the corresponding bit in the address value.
<i>access-list-number</i>	(Optional) Number of a standard IP access list to be applied to incoming routing updates.
ip	(Optional) IP-derived routes for IS-IS. It can be applied independently for IP routes and ISO CLNS routes.

Default

Table 19-1 lists default administrative distances.

Table 19-1 Default Administrative Distances

Route Source	Default Distance
Connected interface	0
Static route	1
External BGP	20
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EGP	140
Internal BGP	200
Unknown	255

Command Mode

Router configuration

Usage Guidelines

Numerically, an administrative distance is an integer between 0 and 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 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 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 “Example” for further clarification).

Weight values are also subjective; there is no quantitative method for choosing weight values.

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

The **show ip protocols** EXEC command displays the default administrative distance for a specified routing process.

Example

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 192.31.7.0 and 128.88.0.0. The first **distance** router configuration command sets the default administrative distance to 255, which instructs the router 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 192.31.7.0 to 90. The third **distance** command sets the administrative distance for the router with the address 128.88.1.3 to 120.

```
router igrp 109
network 192.31.7.0
network 128.88.0.0
distance 255
distance 90 192.31.7.0 0.0.0.255
distance 120 128.88.1.3 0.0.0.0
```

Related Command

distance bgp

distance bgp

To allow the use of external, internal, and local administrative distances that could be a better route to a node, use the **distance bgp** router configuration command. To return to the default values, use the **no** form of this command.

distance bgp *external-distance* *internal-distance* *local-distance*
no distance bgp

Syntax Description

external-distance

Administrative distance for BGP external routes. External routes are routes for which the best path is learned from a neighbor external to the autonomous system. Acceptable values are from 1 to 255. The default is 20. Routes with a distance of 255 are not installed in the routing table.

internal-distance

Administrative distance for BGP internal routes. Internal routes are those routes that are learned from another BGP entity within the same autonomous system. Acceptable values are from 1 to 255. The default is 200. Routes with a distance of 255 are not installed in the routing table.

local-distance

Administrative distance for BGP local routes. Local routes are those networks listed with a **network** router configuration command, often as back doors, for that router or for networks that are being redistributed from another process. Acceptable values are from 1 to 255. The default is 200. Routes with a distance of 255 are not installed in the routing table.

Default

external-distance: 20
internal-distance: 200
local-distance: 200

Command Mode

Router configuration

Usage Guidelines

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 between 0 and 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.

Use this command if another protocol is known to be able to provide a better route to a node than was actually learned via external BGP, or if some internal routes should really be preferred by BGP.

Note Changing the administrative distance of BGP internal routes is considered dangerous and is not recommended. One problem that can arise is the accumulation of routing table inconsistencies, which can break routing.

Example

In the following example, internal routes are known to be preferable to those learned through the IGP, so the administrative distance values are set accordingly:

```
router bgp 109
network 131.108.0.0
neighbor 129.140.6.6 remote-as 123
neighbor 128.125.1.1 remote-as 47
distance bgp 20 20 200
```

Related Command

distance bgp

distance eigrp

To allow the use of two administrative distances—internal and external—that could be a better route to a node, use the **distance eigrp** router configuration command. To reset these values to their defaults, use the **no** form of this command.

```
distance eigrp internal-distance external-distance  
no distance eigrp
```

Syntax Description

internal-distance

Administrative distance for Enhanced IGRP internal routes. Internal routes are those that are learned from another entity within the same autonomous system. It can be a value from 1 to 255.

external-distance

Administrative distance for Enhanced IGRP external routes. External routes are those for which the best path is learned from a neighbor external to the autonomous system. It can be a value from 1 to 255.

Default

internal-distance: 90

external-distance: 170

Command Mode

Router configuration

Usage Guidelines

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 between 0 and 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.

Use the **distance eigrp** command if another protocol is known to be able to provide a better route to a node than was actually learned via external Enhanced IGRP or if some internal routes should really be preferred by Enhanced IGRP.

Table 19-2 lists the default administrative distances.

Table 19-2 Default Administrative Distances

Route Source	Default Distance
Connected interface	0
Static route	1
Enhanced IGRP summary route	5
External BGP	20
Internal enhanced IGRP	90

Route Source	Default Distance
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EGP	140
External enhanced IGRP	170
Internal BGP	200
Unknown	255

To display the default administrative distance for a specified routing process, use the **show ip protocols** EXEC command.

Example

In the following example, the **router eigrp 109** global configuration command sets up Enhanced IGRP routing in autonomous system number 109. The **network** router configuration commands specify Enhanced IGRP routing on networks 192.31.7.0 and 128.88.0.0. The first **distance** router configuration command sets the default administrative distance to 255, which instructs the router to ignore all routing updates from routers for which an explicit distance has not been set. The second **distance** router configuration command sets the administrative distance for all routers on the Class C network 192.31.7.0 to 90. The third **distance** router configuration command sets the administrative distance for the router with the address 128.88.1.3 to 120.

```
router eigrp 109
network 192.31.7.0
network 128.88.0.0
distance 255
!
! use caution when executing the next two commands!
!
distance 90 192.31.7.0 0.0.0.255
distance 120 128.88.1.3 0.0.0.0
```

Related Command

show ip protocols

distribute-list in

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

```
distribute-list access-list-number in [interface-name]  
no distribute-list access-list-number in [interface-name]
```

Syntax Description

<i>access-list-number</i>	Standard IP access list number. 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.
<i>interface-name</i>	(Optional) Interface 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.

Default

Disabled

Command Mode

Router configuration

Usage Guidelines

This command is not supported in IS-IS.

Example

In the following example, the Enhanced IGRP routing process accepts only two networks—network 0.0.0.0 and network 131.108.0.0:

```
access-list 1 permit 0.0.0.0
access-list 1 permit 131.108.0.0
access-list 1 deny 0.0.0.0 255.255.255.255
router eigrp
network 131.108.0.0
distribute-list 1 in
```

Related Commands

A dagger (†) indicates that the command is documented in another chapter.

access-list (standard) [†]
access-list (extended) [†]
distribute-list out
redistribute

distribute-list out

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

```
distribute-list access-list-number out [interface-name | routing-process |
  autonomous-system-number]
no distribute-list access-list-number out [interface-name | routing-process |
  autonomous-system-number]
```

Syntax Description

<i>access-list-number</i>	Standard IP access list number. 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.
<i>interface-name</i>	(Optional) Name of a particular interface.
<i>routing-process</i>	(Optional) Name of a particular routing process, or the keyword static or connected .
<i>autonomous-system-number</i>	(Optional) Autonomous system number.

Default

Disabled

Command Mode

Router configuration

Usage Guidelines

When redistributing networks, a routing process name can be specified as an optional trailing argument to the **distribute-list** command. This 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 131.108.0.0.

```
access-list 1 permit 131.108.0.0
access-list 1 deny 0.0.0.0 255.255.255.255
router rip
network 131.108.0.0
distribute-list 1 out
```

In the following example, access list 1 is applied to outgoing routing updates and IS-IS is enabled on Ethernet interface 0. Only network 131.131.101.0 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 131.131.101.0 0.0.0.255
```

Related Commands

A dagger (†) indicates that the command is documented in another chapter.

access-list (standard) [†]
access-list (extended) [†]
distribute-list in
redistribute

domain-password

To configure the IS-IS routing domain authentication password, use the **domain-password** router configuration command. To disable a password, use the **no** form of this command.

```
domain-password password
  no domain-password [password]
```

Syntax Description

<i>password</i>	Password you assign.
-----------------	----------------------

Default

No password is specified.

Command Mode

Router configuration

Usage Guidelines

This password is inserted in Level 2 (area router level) link state PDUs (LSPs), complete sequence number PDUs (CSNPs), and partial sequence number PDUs (PSNP).

Example

The following example assigns an authentication password to the routing domain:

```
router isis
  domain-password flower
```

Related Command

area-password

ip as-path access-list

To define a BGP-related access list, use the **ip as-path access-list** global configuration command. To disable use of the access list, use the **no** form of this command.

```
ip as-path access-list access-list-number {permit | deny} as-regular-expression
no ip as-path access-list access-list-number {permit | deny} as-regular-expression
```

Syntax Description

access-list-number Integer from 1 to 199 that indicates the regular expression access list number.

permit Permits access for matching conditions.

deny Denies access to matching conditions.

as-regular-expression Autonomous system in the access list using a regular expression. See the “Regular Expressions” appendix for information about forming regular expressions.

Default

No access lists are defined.

Command Mode

Global configuration

Usage Guidelines

You can specify an access list filter on both inbound and outbound BGP routes. In addition, you can assign *weights* based on a set of filters. Each filter is an access list based on regular expressions. If the regular expression matches the representation of the autonomous system path of the route as an ASCII string, then the **permit** or **deny** condition applies. The autonomous system path does not contain the local autonomous system number. Use the **ip as-path access-list** global configuration command to define an BGP access list, and the **neighbor** router configuration command to apply a specific access list.

Example

The following example specifies that the BGP neighbor with IP address 128.125.1.1 is not sent advertisements about any path through or from the adjacent autonomous system 123.

```
ip as-path access-list 1 deny _123_
ip as-path access-list 1 deny ^123$|  
  
router bgp 109
network 131.108.0.0
neighbor 129.140.6.6 remote-as 123
neighbor 128.125.1.1 remote-as 47
neighbor 128.125.1.1 filter-list 1 out
```

Related Commands

neighbor distribute-list
neighbor filter-list

ip community-list

To create a community list for BGP and control access to it, use the **ip community-list** global configuration command. To delete the community list, use the **no** form of this command.

```
ip community-list community-list-number {permit | deny} community-number  
no ip community-list community-list-number
```

Syntax Description

community-list-number Integer 1 through 99 that identifies one or more permit or deny groups of communities.

permit Permits access for a matching condition.

deny Denies access for a matching condition.

community-number Community number configured by a **set community** command. Valid value is one of the following:

- 1 through 4294967200. You can specify a single number or multiple numbers separated by a space.
- **internet**—The Internet community.
- **no-export**—Do not advertise this route to an EBGP peer.
- **no-advertise**—Do not advertise this route to any peer (internal or external).

Default

Once you permit a value for the community number, the community list defaults to an implicit deny for everything else.

Command Mode

Global configuration

Example

In the following example, the router permits all routes except the routes with the communities 5 and 10 or 10 and 15:

```
ip community-list 1 deny 5 10  
ip community-list 1 deny 10 15  
ip community-list 1 permit internet
```

Related Command

set community

ip default-network

To select a network as a candidate route for computing the gateway of last resort, use the **ip default-network** global configuration command. 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.

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 RIP, this is flagged as the pseudonetwork 0.0.0.0; for IGRP, it is the network itself, flagged as an exterior route.

Command Mode

Global configuration

Usage Guidelines

The router 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 **ip default-network**) 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 non-zero 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 10.0.0.0 255.0.0.0 131.108.3.4
ip default-network 10.0.0.0
```

If the following command was issued on a router not connected to network 129.140.0.0, the router might choose the path to that network as a default route when the network appeared in the routing table:

```
ip default-network 129.140.0.0
```

Related Command

show ip route

ip dvmrp accept-filter

To configure an acceptance filter for incoming DVMRP reports, use the **ip dvmrp accept-filter** interface configuration command. To disable this feature, use the **no** form of this command.

```
ip dvmrp accept-filter access-list-number [distance]  
no ip dvmrp accept-filter access-list-number [distance]
```

Syntax Description

<i>access-list-number</i>	Number of a standard IP access list. This can be a number from 0 to 99. A value of 0 means that all sources are accepted with the configured distance.
<i>distance</i>	(Optional) Administrative distance to the destination.

Default

All destinations are accepted with a distance of 0.

Command Mode

Interface configuration

Usage Guidelines

Any sources that match the access list are stored in the DVMRP routing table with *distance*.

The *distance* is used to compare with the same source in the unicast routing table. The route with the lower distance (either the route in the unicast routing table or that in the DVMRP routing table) takes precedence when computing the Reverse Path Forwarding (RPF) interface for a source of a multicast packet.

By default, the administrative distance for DVMRP routes is 0. This means that they always take precedence over unicast routing table routes. If you have two paths to a source, one through unicast routing (using PIM as the multicast routing protocol) and another path using DVMRP (unicast and multicast routing), and if you want to use the PIM path, use the **ip dvmrp accept-filter** command to increase the administrative distance for DVMRP routes. For example, if the unicast routing protocol is Enhanced IGRP, which has a default administrative distance of 90, you could define and apply the following access list so the RPF interface used to accept multicast packets will be through the Enhanced IGRP/PIM path:

```
ip dvmrp accept-filter 1 100  
access-list 1 permit 0.0.0.0 255.255.255.255
```

Example

The following example applies access list 57 to the interface and sets a distance of 4:

```
access-list 57 permit 131.108.0.0 0.0.255.255  
access-list 57 permit 198.92.37.0 0.0.0.255  
access-list 57 deny 0.0.0.0 255.255.255.255  
ip dvmrp accept-filter 57 4
```

Related Commands

A dagger (†) indicates that the command is documented in another chapter.

distance

ip dvmrp metric

show ip dvmrp route

tunnel mode †

ip dvmrp default-information

To advertise network 0.0.0.0 to DVMRP neighbors on an interface, use the **ip dvmrp default-information** interface configuration command. To prevent the advertisement, use the **no** form of this command.

```
ip dvmrp default-information {originate | only}  
no ip dvmrp default-information {originate | only}
```

Syntax Description

originate	Other routes more specific than 0.0.0.0 can also be advertised.
only	No DVMRP routes other than 0.0.0.0 are advertised.

Default

Disabled

Command Mode

Interface configuration

Usage Guidelines

This command should only be used when the router is a neighbor to mrouted version 3.6 machines. The mrouted protocol is a public domain implementation of DVMRP.

You can use the **ip dvmrp metric** command with the **ip dvmrp default-information** command to tailor the metric used when advertising the default route 0.0.0.0. By default, metric 1 is used.

Example

The following example configures the router to advertise network 0.0.0.0, in addition to other networks, to DVMRP neighbors:

```
ip dvmrp default-information originate
```

Related Command

ip dvmrp metric

ip dvmrp metric

To configure the metric associated with a set of destinations for DVMRP reports, use the **ip dvmrp metric** interface configuration command. To disable this function, use the **no** form of this command.

```
ip dvmrp metric metric [list access-list-number] [protocol process-id] | [dvmrp]
no ip dvmrp metric metric [list access-list-number] [protocol process-id] | [dvmrp]
```

Syntax Description

<i>metric</i>	Metric associated with a set of destinations for DVMRP reports. It can be a value from 0 to 32. A value of 0 means that the route is not advertised. A value of 32 is equivalent to infinity (unreachable).
list <i>access-list-number</i>	(Optional) Number of an access list. If you specify this argument, only the multicast destinations that match the access list are reported with the configured metric. Any destinations not advertised because of split horizon do not use the configured metric.
protocol	(Optional) Name of unicast routing protocol. It can be bgp , egp , eigrp , igrp , isis , ospf , rip , or static . (Note that these are the protocol names you can specify with a router protocol command.) If you specify these arguments, only routes learned by the specified routing protocol are advertised in DVMRP report messages.
process-id	(Optional) Process ID number of the unicast routing protocol.
dvmrp	(Optional) Allows routes from the DVMRP routing table to be advertised with the configured <i>metric</i> or filtered.

Default

No metric is preconfigured. Only directly connected subnets and networks are advertised to neighboring DVMRP routers.

Command Mode

Interface configuration

Usage Guidelines

When PIM is configured on an interface and DVMRP neighbors are discovered, the router sends DVMRP report messages for directly connected networks. The **ip dvmrp metric** command enables DVMRP report messages for multicast destinations that match the access list. Usually, the metric for these routes is 1. Under certain circumstances, it may be desirable to tailor the metric used for various unicast routes.

Use the *access-list-number* argument in conjunction with the *protocol process-id* arguments to selectively list the destinations learned from a given routing protocol.

To display DVMRP activity, use the **debug ip dvmrp** command.

Example

The following example connects a PIM cloud to a DVMRP cloud. Access list 1 permits the sending of DVMRP reports to the DVMRP routers advertising all sources in the 198.92.35.0 network with a metric of 1. Access list 2 permits all other destinations, but the metric of 0 means that no DVMRP reports are sent for these destinations.

```
access-list 1 permit 198.92.35.0 0.0.0.255
access-list 1 deny 0.0.0.0 255.255.255.255
access-list 2 permit 0.0.0.0 255.255.255.255
interface tunnel 0
ip dvmrp metric 1 list 1
ip dvmrp metric 0 list 2
```

Related Commands

Two daggers (††) indicate that the command is documented in the *Debug Command Reference* publication.

debug ip dvmrp ††
ip dvmrp accept-filter

ip gdp

To enable GDP routing on an interface, use the **ip gdp** interface configuration command. To disable GDP routing, use the **no** form of this command.

```
ip gdp [priority number | reporttime seconds | holdtime seconds]  
no ip gdp
```

Syntax Description

priority <i>number</i>	(Optional) Alters the GDP priority; default is a priority of 100. A larger number indicates a higher priority.
reporttime <i>seconds</i>	(Optional) Alters the GDP reporting interval; the default is 5 seconds for broadcast media such as Ethernets, and never for nonbroadcast media such as X.25.
holdtime <i>seconds</i>	(Optional) Alters the GDP default hold time of 15 seconds.

Default

priority: 100
reporttime: 5 seconds for broadcast media; 0 for nonbroadcast media
holdtime: 15 seconds

Command Mode

Interface configuration

Usage Guidelines

When enabled on an interface, GDP updates report the primary and secondary IP addresses of that interface.

Example

In the following example, GDP is enabled on Ethernet interface 1 with a report time of 10 seconds, and priority and hold time set to their defaults (because none are specified):

```
ip gdp reporttime 10
```

ip hello-interval eigrp

To configure the hello interval for the Enhanced IGRP routing process designated by an autonomous system number, use the **ip hello-interval eigrp** interface configuration command. To restore the default value, use the **no** form of this command.

ip hello-interval eigrp *autonomous-system-number* *seconds*
no ip hello-interval eigrp *autonomous-system-number* *seconds*

Syntax Description

autonomous-system-number Autonomous system number.

seconds Hello interval, in seconds.

Default

For low-speed, NBMA networks: 60 seconds

For all other networks: 5 seconds

Command Mode

Interface configuration

Usage Guidelines

The default of 60 seconds applies only to low speed, nonbroadcast, multiaccess (NBMA) media. Low speed is considered to be a rate of T1 or slower, as specified with the **bandwidth** interface configuration command. Note that for the purposes of Enhanced IGRP, Frame Relay and SMDS networks may or may not be considered to be NBMA. These networks are considered NBMA if the interface has not been configured to use physical multicasting; otherwise they are considered not to be NBMA.

Example

The following example sets the hello interval for Ethernet interface 0 to 10 seconds:

```
interface ethernet 0
  ip hello-interval eigrp 109 10
```

Related Command

ip hold-time eigrp

ip hold-time eigrp

To configure the hold time for a particular Enhanced IGRP routing process designated by the autonomous system number, use the **ip hold-time eigrp** interface configuration command. To restore the default value, use the **no** form of this command.

ip hold-time eigrp *autonomous-system-number* *seconds*
no ip hold-time eigrp *autonomous-system-number* *seconds*

Syntax Description

autonomous-system-number Autonomous system number.
seconds Hold time, in seconds.

Default

For low-speed, NBMA networks: 180 seconds

For all other networks: 15 seconds

Command Mode

Interface configuration

Usage Guidelines

On very congested and large networks, the default hold time might not be sufficient time for all routers to receive hello packets from their neighbors. In this case, you may want to increase the hold time.

The hold time is three times the hello interval. If the current value for the hold time is less than two times the hello interval, the hold time is reset.

If a router does not receive a hello packet within the specified hold time, routes through the router are considered available.

Increasing the hold time delays route convergence across the network.

The default of 180 seconds applies only to low speed, nonbroadcast, multiaccess (NBMA) media. Low speed is considered to be a rate of T1 or slower, as specified with the **bandwidth** interface configuration command.

Example

The following example sets the hold time for Ethernet interface 0 to 40 seconds:

```
interface ethernet 0
 ip hold-time eigrp 109 40
```

Related Command

ip hello-interval eigrp

ip igmp access-group

To control the multicast groups that hosts on the subnet serviced by an interface can join, use the **ip igmp access-group** interface configuration command. To disable groups on an interface, use the **no** form of this command.

```
ip igmp access-group access-list-number
no ip igmp access-group access-list-number
```

Syntax Description

<i>access-list-number</i>	Number of a standard IP access list. This can be a number from 1 to 99.
---------------------------	---

Default

All groups are allowed on an interface.

Command Mode

Interface configuration

Example

In the following example, hosts serviced by Ethernet interface 0 can join the group 225.2.2.2 only:

```
access-list 1 225.2.2.2 0.0.0.0
interface ethernet 0
ip igmp access-group 1
```

Related Command

ip igmp join-group

ip igmp join-group

To have the router join a multicast group, use the **ip igmp join-group** interface configuration command. To cancel membership in a multicast group, use the **no** form of this command.

ip igmp join-group *group-address*
no ip igmp join-group *group-address*

Syntax Description

group-address Address of the multicast group. This is a multicast IP address in four-part dotted notation.

Default

No multicast group memberships are predefined.

Command Mode

Interface configuration

Usage Guidelines

IP packets that are addressed to the group address are passed to the IP client process in the router.

If all the multicast-capable routers that you administer are members of a multicast group, pinging that group causes all routers to respond. This can be a useful administrative and debugging tool.

Another reason to have a router join a multicast group is when other hosts on the network have a bug in IGRP that prevents them from correctly answering IGMP queries. Having the router join the multicast group causes upstream routers to maintain multicast routing table information for that group and keep the paths for that group active.

Example

In the following example, the router joins multicast group 225.2.2.2:

```
ip igmp join-group 225.2.2.2
```

Related Commands

A dagger (†) indicates that the command is documented in another chapter.

ip igmp access-group
ping (privileged) †
ping (user) †

ip igmp query-interval

To configure the frequency at which the router sends IGMP host-query messages, use the **ip igmp query-interval** interface configuration command. To return to the default frequency, use the **no** form of this command.

```
ip igmp query-interval seconds
no ip igmp query-interval
```

Syntax Description

<i>seconds</i>	Frequency, in seconds, at which to transmit IGMP host-query messages. The can be a number from 0 to 65535. The default is 60 seconds.
----------------	---

Default

60 seconds

Command Mode

Interface configuration

Usage Guidelines

Multicast routers send host membership query messages (referred to as host-query messages) to discover which multicast groups have members on the router's attached networks. Hosts respond with IGMP report messages indicating that they wish to receive multicast packets for specific groups (that is, indicating that the host wants to become a member of the group). Host-query messages are addressed to the all-hosts multicast group, which has the address 224.0.0.1, and have an IP TTL value of 1.

The designated router for a LAN is the only router that sends IGMP host-query messages. The designated router is elected according to the multicast routing protocol that runs on the LAN.

Note Changing this value may severely impact multicast forwarding.

Example

The following example changes the frequency at which the designated router sends IGMP host-query messages to 2 minutes:

```
interface tunnel 0
ip igmp query-interval 120
```

Related Commands

ip pim query-interval
show ip igmp groups

ip irdp

To enable ICMP Router Discovery Protocol (IRDP) processing on an interface, use the **ip irdp** interface configuration command. To disable IRDP routing, use the **no** form of this command.

```
ip irdp [multicast | holdtime seconds | maxadvertinterval seconds | minadvertinterval
seconds | preference number | address address [number]]
no ip irdp
```

Syntax Description

multicast	(Optional) Use the multicast address (224.0.0.1) instead of IP broadcasts.
holdtime seconds	(Optional) Length of time in seconds advertisements are held valid. Default is three times the maxadvertinterval value. Must be greater than maxadvertinterval and cannot be greater than 9000 seconds.
maxadvertinterval seconds	(Optional) Maximum interval in seconds between advertisements. The default is 600 seconds.
minadvertinterval seconds	(Optional) Minimum interval in seconds between advertisements. The default is 0.75 times the maxadvertinterval . If you change the maxadvertinterval value, this value defaults to three-quarters of the new value.
preference number	(Optional) Router's preference value. The allowed range is -2^{31} to 2^{31} . The default is 0. A higher value increases the router's preference level. You can modify a particular router so that it will be the preferred router to which others home.
address address [number]	(Optional) IP address (<i>address</i>) to proxy-advertise, and optionally, its preference value (<i>number</i>).

Default

Disabled

When enabled, IRDP uses these defaults:

- Broadcast IRDP advertisements
- Maximum interval between advertisements: 600 seconds
- Minimum interval between advertisements: 0.75 times **maxadvertinterval**
- Preference: 0

Command Mode

Interface configuration

Usage Guidelines

If you change **maxadvertinterval**, the other two values also change, so it is important to change **maxadvertinterval** first before changing either **holdtime** or **minadvertinterval**.

The **ip irdp multicast** command allows for compatibility with Sun Microsystems Solaris, which requires IRDP packets to be sent out as multicasts. Many implementations cannot receive these multicasts; ensure end host ability before using this command.

Example

The following example illustrates how to set the various IRDP processes:

```
! enable irdp on interface Ethernet 0
interface ethernet 0
ip irdp
! send IRDP advertisements to the multicast address
ip irdp multicast
! increase router preference from 100 to 50
ip irdp preference 50
! set maximum time between advertisements to 400 secs
ip irdp maxadvertinterval 400
! set minimum time between advertisements to 100 secs
ip irdp minadvertinterval 100
! advertisements are good for 6000 seconds
ip irdp holdtime 6000
! proxy-advertise 131.108.14.5 with default router preference
ip irdp address 131.108.14.5
! proxy-advertise 131.108.14.6 with preference of 50
ip irdp address 131.108.14.6 50
```

ip mroute

To configure a multicast static route (mroute), use the **ip mroute** global configuration command. To remove the route, use the **no** form of this command.

ip mroute *source mask [protocol as-number] {rpf-address | type number} [distance]*
no ip mroute *source mask [protocol as-number] {rpf-address | type number} [distance]*

Syntax Description

<i>source</i>	IP address of the multicast source.
<i>mask</i>	Mask on the IP address of the multicast source.
<i>protocol</i>	(Optional) Unicast routing protocol that you are using.
<i>as-number</i>	(Optional) Autonomous system number of the routing protocol you are using, if applicable.
<i>rpf-address</i>	Incoming interface for the mroute. If the Reverse Path Forwarding address <i>rpf-address</i> is a PIM neighbor, PIM Joins, Grafts, and Prunes are sent to it. The <i>rpf-address</i> can be a host IP address of a directly connected system or a network/subnet number. When it is a route, a recursive lookup is done from the unicast routing table to find a directly connected system. If <i>rpf-address</i> is not specified, the interface <i>type number</i> is used as the incoming interface.
<i>type number</i>	Interface type and number for the mroute.
<i>distance</i>	(Optional) Determines whether a unicast route, a DVMRP route, or a static mroute should be used for the RPF lookup. The lower distances have better preference. If the static mroute has the same distance as the other two RPF sources, the static mroute will take precedence. The default is 0.

Default

distance: 0

Command Mode

Global configuration

Usage Guidelines

This command allows you to statically configure where multicast sources are located (even though the unicast routing table says something different).

When a source range is specified, the *rpf-address* applies only to those sources.

Examples

The following example configures all sources via a single interface (in this case, a tunnel):

```
ip mroute 0.0.0.0 255.255.255.255 tunnel0
```

The following example configures all specific sources within a network number are reachable through 171.68.10.13:

```
ip mroute 171.69.0.0 255.255.0.0 171.68.10.13
```

The following example causes this multicast static route to take effect if the unicast routes for any given destination go away:

```
ip mroute 0.0.0.0 255.255.255.255 serial0 200
```

ip mroute-cache

To configure IP multicast fast switching, use the **ip mroute-cache** interface configuration command. To disable IP multicast fast switching, use the **no** form of this command.

```
ip mroute-cache
no ip mroute-cache
```

Syntax Description

This command has no arguments or keywords.

Default

Enabled

Command Mode

Interface configuration

Usage Guidelines

If fast switching is disabled on an incoming interface for a multicast routing table entry, the packet will be sent at process level for all interfaces in the outgoing interface list.

If fast switching is disabled on an outgoing interface for a multicast routing table entry, the packet is process level switched for that interface, but might be fast-switched for other interfaces in the outgoing interface list.

When fast switching is enabled (like unicast routing), debug messages are not logged. If you want to log debug messages, disable fast switching.

Example

The following example disables IP multicast fast switching on the interface:

```
no ip mroute-cache
```

ip multicast rate-limit

To control the rate a sender from the source-list can send to a multicast group in the group-list, use the **ip multicast rate-limit** interface configuration command. To remove the control, use the **no** form of this command.

```
ip multicast rate-limit {in | out} [group-list access-list] [source-list access-list] kbps
no multicast rate-limit {in | out} [group-list access-list] [source-list access-list] kbps
```

Syntax Description

in	Only packets at the rate of <i>kbps</i> or slower are accepted on the interface.
out	Only a maximum of <i>kbps</i> will be transmitted on the interface.
group-list access-list	(Optional) Specifies the access list number that controls which multicast groups are subject to the rate limit.
source-list access-list	(Optional) Specifies the access list number that controls which senders are subject to the rate limit.
<i>kbps</i>	Kilobits per second transmission rate.

Default

kbps = 0, meaning that there is no limit on the rate traffic is sent.

Command Mode

Interface configuration

Usage Guidelines

If a router receives a packet and in the last second the user has sent over the limit, the packet is dropped; otherwise, it is forwarded.

Example

In the following example, packets to any group from sources in network 171.69.0.0 will have their packets rate-limited to 64 kilobits per second:

```
interface serial 0
ip multicast rate-limit out group-list 1 source-list 2 64
access-list 1 permit 0.0.0.0 255.255.255.255
access-list 2 permit 171.69.0.0 0.0.255.255
```

ip multicast-routing

To enable IP multicast routing on the router, use the **ip multicast-routing** global configuration command. To disable IP multicast routing, use the **no** form of this command.

```
ip multicast-routing
no ip multicast-routing
```

Syntax Description

This command has no arguments or keywords.

Default

Disabled

Command Mode

Global configuration

Usage Guidelines

When IP multicast routing is disabled, the router does not forward any multicast packets.

Example

The following example enables IP multicast routing on the router:

```
ip multicast-routing
```

Related Command

ip pim

ip multicast ttl-threshold

To configure the time-to-live (TTL) threshold of packets being forwarded out an interface, use the **ip multicast ttl-threshold** interface configuration command. To return to the default TTL threshold, use the **no** form of this command.

```
ip multicast ttl-threshold ttl
no ip multicast ttl-threshold [ttl]
```

Syntax Description

ttl

Time-to-live value, in hops. It can be a value from 0 to 255. The default value is 0, which means that all multicast packets are forwarded out the interface.

Default

0, which means that all multicast packets are forwarded out the interface.

Command Mode

Interface configuration

Usage Guidelines

Only multicast packets with a TTL value greater than the threshold are forwarded out the interface.

You should configure the TTL threshold only on border routers. Conversely, routers on which you configure a TTL threshold value automatically become border routers.

This command replaces the **ip multicast-threshold** command, which is obsolete.

Example

In the following example, you set the TTL threshold on a border router to 200, which is a very high value. This means that multicast packets must have a TTL greater than 200 in order to be forwarded out this interface. Multicast applications generally set this value well below 200. Therefore, setting a value of 200 means that no packets will be forwarded out the interface.

```
interface tunnel 0
ip multicast ttl-threshold 200
```

ip ospf authentication-key

To assign a password to be used by neighboring routers that are using OSPF's simple password authentication, use the **ip ospf authentication-key** interface configuration command. To remove a previously assigned OSPF password, use the **no** form of this command.

```
ip ospf authentication-key password
no ip ospf authentication-key
```

Syntax Description

<i>password</i>	Any continuous string of characters that can be entered from the keyboard up to 8 bytes in length.
-----------------	--

Default

No password is specified.

Command Mode

Interface configuration

Usage Guidelines

The password created by this command is used as a “key” that is inserted directly into the OSPF header when the router originates routing protocol packets. A separate password can be assigned to each network on a per-interface basis. All neighboring routers on the same network must have the same password to be able to exchange OSPF information.

Note A router will use this key only when authentication is enabled for an area with the **area authentication** router configuration command.

Example

In the following example, the authentication key is enabled with the string *yourpass*:

```
ip ospf authentication-key yourpass
```

Related Command

area authentication

ip ospf cost

To explicitly specify the cost of sending a packet on an interface, use the **ip ospf cost** interface configuration command. To reset the path cost to the default value, use the **no** form of this command.

```
ip ospf cost cost  
no ip cost
```

Syntax Description

<i>cost</i>	Unsigned integer value expressed as the link state metric. It can be a value in the range 1 to 65535.
-------------	---

Default

No default cost is predefined.

Command Mode

Interface configuration

Usage Guidelines

Unlike IGRP, you must set this metric manually using this command, if you need to change the default. Changing the bandwidth does not change the link cost.

The link state metric is advertised as the link cost in the router's router link advertisement. We do not support type of service (TOS), so you can assign only one cost per interface.

In general, the path cost is calculated using the following formula:

$$10^8 \frac{\text{Bandwidth}}{\text{Delay}}$$

Using the above formula, the default path costs were calculated as noted in the following list. If these values do not suit your network, you can use your own method of calculating path costs.

- 56-kbps serial link—Default cost is 1785
- 64-kbps serial link—Default cost is 1562
- T1 (1.544-Mbps serial link)—Default cost is 65
- E1 (2.048-Mbps serial link)—Default cost is 48
- 4-Mbps Token Ring—Default cost is 25
- Ethernet—Default cost is 10
- 16-Mbps Token Ring—Default cost is 6
- FDDI—Default cost is 1

Example

The following example sets the interface cost value to 65:

```
ip ospf cost 65
```

ip ospf dead-interval

To set how long a router's Hello packets must not have been seen before its neighbors declare the router down, use the **ip ospf dead-interval** interface configuration command. To return to the default time, use the **no** form of this command.

```
ip ospf dead-interval seconds
no ip ospf dead-interval
```

Syntax Description

<i>seconds</i>	Unsigned integer that specifies the interval in seconds; the value must be the same for all nodes on the network.
----------------	---

Default

Four times the interval set by the **ip ospf hello-interval** command

Command Mode

Interface configuration

Usage Guidelines

The interval is advertised in the router's Hello packets. This value must be the same for all routers on a specific network.

Example

The following example sets the OSPF dead interval to 60 seconds:

```
interface ethernet 1
  ip ospf dead-interval 60
```

Related Command

ip ospf hello-interval

ip ospf hello-interval

To specify the interval between Hello packets that the router sends on the interface, use the **ip ospf hello-interval** interface configuration command. To return to the default time, use the **no** form of this command.

ip ospf hello-interval *seconds*
no ip ospf hello-interval

Syntax Description

seconds Unsigned integer that specifies the interval in seconds. The value must be the same for all nodes on a specific network.

Default

10 seconds

Command Mode

Interface configuration

Usage Guidelines

This value is advertised in the router's Hello packets. The smaller the Hello interval, the faster topological changes will be detected, but more routing traffic will ensue. This value must be the same for all routers on a specific network.

Example

The following example sets the interval between Hello packets to 15 seconds:

```
interface ethernet 1
  ip ospf hello-interval 15
```

Related Command

ip ospf dead-interval

ip ospf message-digest-key

To enable OSPF MD5 authentication, use the **ip ospf message-digest-key** interface configuration command. To remove an old MD5 key, use the **no** form of this command.

ip ospf message-digest-key *keyid* md5 *key*
no ip ospf message-digest-key *keyid*

Syntax Description

<i>keyid</i>	An identifier in the range 1 through 255.
<i>key</i>	Alphanumeric password of up to 16 bytes.

Default

OSPF MD5 authentication is disabled.

Command Mode

Interface configuration

Usage Guidelines

Usually there is one key per interface, which is used to generate authentication information when sending packets and to authenticate incoming packets. The same key identifier on the neighbor router must have the same *key* value.

The process of changing keys is as follows. Suppose the current configuration is as follows:

```
interface ethernet 1
  ip ospf message-digest-key 100 md5 OLD
```

You change the configuration to the following:

```
interface ethernet 1
  ip ospf message-digest-key 101 md5 NEW
```

The system assumes its neighbors do not have the new key yet, so it begins a rollover process. It sends multiple copies of the same packet, each authenticated by different keys. In this example, the system sends out two copies of the same packet—the first one authenticated by key 100 and the second one authenticated by key 101.

Rollover allows neighboring routers to continue communication while the network administrator is updating them with the new key. Rollover stops once the local system finds that all its neighbors know the new key. The system detects that a neighbor has the new key when it receives packets from the neighbor authenticated by the new key.

After all neighbors have been updated with the new key, the old key should be removed. In this example, you would enter the following:

```
interface ethernet 1
  no ip ospf message-digest-key 100
```

Then, only key 101 is used for authentication on Ethernet interface 1.

We recommend that you not keep more than one key per interface. Every time you add a new key, you should remove the old key to prevent the local system from continuing to communicate with a hostile system that knows the old key. Removing the old key also reduces overhead during rollover.

Example

The following example sets a new key 19 with the password *8ry4222*:

```
interface ethernet 1
  ip ospf message-digest-key 10 md5 xvv560qle
  ip ospf message-digest-key 19 md5 8ry4222
```

Related Command

area authentication

ip ospf name-lookup

To configure OSPF to look up Domain Name System (DNS) names for use in all OSPF **show** EXEC command displays, use the **ip ospf name-lookup** global configuration command. To disable this feature, use the **no** form of this command.

```
ip ospf name-lookup
no ip ospf name-lookup
```

Syntax Description

This command has no arguments or keywords.

Default

Disabled

Command Mode

Global configuration

Usage Guidelines

This feature makes it easier to identify a router because it is displayed by name rather than by its router ID or neighbor ID.

Example

The following example configures OSPF to look up DNS names for use in all OSPF **show** EXEC command displays:

```
ip ospf name-lookup
```

Sample Display

The following is sample output from the **show ip ospf database** EXEC command, for example, once you have enabled the DNS name lookup feature.

```
Router# show ip ospf database

OSPF Router with id (160.89.41.1) (Autonomous system 109)

Router Link States (Area 0.0.0.0)

Link ID      ADV Router      Age      Seq#      Checksum Link count
160.89.41.1  router        381      0x80000003 0x93BB    4
160.89.34.2  neon          380      0x80000003 0xD5C8    2

Net Link States (Area 0.0.0.0)

Link ID      ADV Router      Age      Seq#      Checksum
160.89.32.1  router        381      0x80000001 0xC117
```

ip ospf network

To configure the OSPF network type to a type other than the default for a given media, use the **ip ospf network** interface configuration command. To return to the default value, use the **no** form of this command.

```
ip ospf network {broadcast | non-broadcast | point-to-multipoint}  
no ip ospf network
```

Syntax Description

broadcast	Sets the network type to broadcast.
non-broadcast	Sets the network type to nonbroadcast.
point-to-multipoint	Sets the network type to point-to-multipoint.

Default

Depends on the network type

Command Mode

Interface configuration

Usage Guidelines

Using this feature, you can configure broadcast networks as nonbroadcast multiaccess networks when, for example, you have routers in your network that do not support multicast addressing. You can also configure nonbroadcast multiaccess networks, such as X.25, Frame Relay, and SMDS, as broadcast networks. This feature saves you from having to configure neighbors.

Configuring nonbroadcast multiaccess networks as either broadcast or nonbroadcast assumes that there are virtual circuits from every router to every router or fully-meshed network. This is not true for some cases, for example, due to cost constraints or when you have only a partially-meshed network. In these cases, you can configure the OSPF network type as a point-to-multipoint network. Routing between two routers that are not directly connected will go through the router that has virtual circuits to both routers. Note that you do not need to configure neighbors when using this feature.

If this command is issued on an interface that does not allow it, it will be ignored.

Example

The following example sets your OSPF network as a broadcast network:

```
interface serial 0  
ip address 160.89.77.17 255.255.255.0  
ip ospf network broadcast  
encapsulation frame-relay
```

Related Commands

A dagger (†) indicates that the command is documented in another chapter.

frame-relay map †

neighbor (OSPF)

x25 map †

ip ospf priority

To set the router's priority, which helps determine the designated router for this network, use the **ip ospf priority** interface configuration command. To return to the default value, use the **no** form of this command.

ip ospf priority *number*
no ip ospf priority

Syntax Description

number 8-bit unsigned integer that specifies the priority. The range is from 0 to 255.

Default

Priority of 1

Command Mode

Interface configuration

Usage Guidelines

When two routers attached to a network both attempt to become the designated router, the one with the higher router priority takes precedence. If there is a tie, the router with the higher router ID takes precedence. A router with a router priority set to zero is ineligible to become the designated router or backup designated router. Router priority is only configured for interfaces to multiaccess networks (in other words, not point-to-point networks).

This priority value is used when you configure OSPF for nonbroadcast networks using the **neighbor** router configuration command for OSPF.

Example

The following example sets the router priority value to 4:

```
interface ethernet 0
  ip ospf priority 4
```

Related Commands

ip ospf network
neighbor (OSPF)

ip ospf retransmit-interval

To specify the time between link state advertisement retransmissions for adjacencies belonging to the interface, use the **ip ospf retransmit-interval** interface configuration command. To return to the default value, use the **no** form of this command.

```
ip ospf retransmit-interval seconds
no ip ospf retransmit-interval
```

Syntax Description

<i>seconds</i>	Time in seconds between retransmissions. It must be greater than the expected round-trip delay between any two routers on the attached network. The range is 1 to 65535 seconds. The default is 5 seconds.
----------------	--

Default

5 seconds

Command Mode

Interface configuration

Usage Guidelines

When a router sends a link state advertisement (LSA) to its neighbor, it keeps the LSA until it receives back the acknowledgment. If it receives no acknowledgment in *seconds*, it will retransmit the LSA.

The setting of this parameter should be conservative, or needless retransmission will result. The value should be larger for serial lines and virtual links.

Example

The following example sets the retransmit-interval value to 8 seconds:

```
interface ethernet 2
ip ospf retransmit-interval 8
```

ip ospf transmit-delay

To set the estimated time it takes to transmit a link state update packet on the interface, use the **ip ospf transmit-delay** interface configuration command. To return to the default value, use the **no** form of this command.

```
ip ospf transmit-delay seconds
no ip ospf transmit-delay
```

Syntax Description

seconds Time in seconds that it takes to transmit a link state update. It can be an integer in the range is 1 to 65535 seconds. The default is 1 second.

Default

1 second

Command Mode

Interface configuration

Usage Guidelines

Link state advertisements in the update packet must have their age incremented by the amount specified in the *seconds* argument before transmission. The value assigned should take into account the transmission and propagation delays for the interface.

If the delay is not added before transmission over a link, the time in which the LSA propagates over the link is not considered. This setting has more significance on very low speed links.

Example

The following example sets the retransmit-delay value to 3 seconds:

```
interface ethernet 0
  ip ospf transmit-delay 3
```

ip pim

To enable PIM on an interface, use the **ip pim** interface configuration command. To disable PIM on the interface, use the **no** form of this command.

```
ip pim {dense-mode | sparse-mode}
no ip pim {dense-mode | sparse-mode}
```

Syntax Description

dense-mode Enables dense mode of operation.

sparse-mode Enables sparse mode of operation.

Default

IP multicast routing is disabled on all interfaces.

Command Mode

Interface configuration

Usage Guidelines

Enabling PIM on an interface also enables IGMP operation on that interface. An interface can be configured to be in dense mode or sparse mode. The mode describes how the router populates its multicast routing table and how the router forwards multicast packets it receives from its directly connected LANs. In populating the multicast routing table, dense-mode interfaces are always added to the table. Sparse-mode interfaces are added to the table only when periodic join messages are received from downstream routers or there is a directly connected member on the interface.

Initially, a dense-mode interface forwards multicast packets until the router determines that there are group members or downstream routers, or until a prune message is received from a downstream router. Then, the dense-mode interface will periodically forward multicast packets out the interface until the same conditions occur. Dense mode assumes that there are multicast group members present. Dense-mode routers never send a join message. They do send prune messages as soon as they determine they have no members or downstream PIM routers. A dense-mode interface is subject to multicast flooding by default.

A sparse-mode interface is used for multicast forwarding only if a join message is received from a downstream router or if there are group members directly connected to the interface. Sparse mode assumes that there are no other multicast group members present. When sparse-mode routers want to join the shared path, they periodically send join messages toward the RP. When sparse-mode routers want to join the source path, they periodically send join messages toward the source; they also send periodic prune messages toward the RP to prune the shared path.

Examples

The following commands enables sparse-mode PIM on tunnel interface 0 and sets the address of the RP router to 226.0.0.8:

```
interface tunnel 0
ip pim sparse-mode
ip pim rp-address 226.0.0.8
```

The following commands enable dense-mode PIM on Ethernet interface 1:

```
interface ethernet 1
  ip pim dense-mode
```

Related Commands

ip multicast-routing
ip pim rp-address
show ip pim interface

ip pim nbma-mode

To configure a multiaccess WAN interface to be in nonbroadcast, multiaccess mode, use the **ip pim nbma-mode** interface configuration command. To disable this feature, use the **no** form of this command.

```
ip pim nbma-mode
no pim nbma-mode
```

Syntax Description

This command has no arguments or keywords.

Default

Disabled

Command Mode

Interface configuration

Usage Guidelines

Use this command on Frame Relay, SMDS, or ATM only, especially when these media do not have native multicast available. Do not use this command on multicast-capable LANs such as Ethernet or FDDI.

When this command is configured, each PIM Join message is kept track of in the outgoing interface list of a multicast routing table entry. Therefore, only PIM WAN neighbors that have joined for the group will get packets sent as data link unicasts. This command should only be used when **ip pim sparse-mode** is configured on the interface. This command is not recommended for LANs that have natural multicast capabilities.

Example

The following example configures an interface to be in nonbroadcast, multiaccess mode:

```
ip pim nbma-mode
```

Related Command

ip pim sparse-mode

ip pim query-interval

To configure the frequency of PIM router-query messages, use the **ip pim query-interval** interface configuration command. To return to the default interval, use the **no** form of this command.

```
ip pim query-interval seconds
no ip pim query-interval [seconds]
```

Syntax Description

<i>seconds</i>	Interval, in seconds, at which periodic PIM router-query messages are sent. It can be a number from 1 to 65535. The default is 30 seconds.
----------------	--

Default

30 seconds

Command Mode

Interface configuration

Usage Guidelines

Routers that are configured for IP multicast send PIM router-query messages to determine which router will be the designated router for each LAN segment (subnet). The designated router is responsible for sending IGMP host-query messages to all hosts on the directly connected LAN. When operating in sparse mode, the designated router is responsible for sending source registration messages to the RP. The designated router is the router with the largest IP address.

Example

The following example changes the PIM router-query message interval to 45 seconds:

```
interface tunnel 0
ip pim query-interval 45
```

Related Command

ip igmp query-interval

ip pim rp-address

To configure the address of a PIM rendezvous point (RP) for a particular group, use the **ip pim rp-address** global configuration command. To remove an RP address, use the **no** form of this command.

ip pim rp-address *ip-address* [*access-list-number*]
no ip pim rp-address *ip-address* [*access-list-number*]

Syntax Description

<i>ip-address</i>	IP address of a router to be a PIM RP. This is a unicast IP address in four-part dotted notation.
<i>access-list-number</i>	(Optional) Number of an access list that defines which multicast groups the RP should be used for. This is a standard IP access list. The number can be from 1 to 100.

Default

No PIM RPs are preconfigured.

Command Mode

Global configuration

Usage Guidelines

You must configure the IP address of RPs in leaf routers only. Leaf routers are those routers that are directly connected either to a multicast group member or to a sender of multicast messages.

The RP address is used by first-hop routers to send register packets on behalf of source multicast hosts to the RP. This address is also used by routers on behalf of multicast hosts that want to become members of a group to send join messages towards the RP. The RP must be a PIM router; however, it does not require any special configuration to recognize that it is the RP. Also, RPs are not members of the multicast group; rather, they serve as a “meeting place” for multicast sources and group members.

Choosing the router that will be an RP requires prior coordination between the people who want to be members of the multicast group. You should examine the length of the paths between members and sources. Remember that most multicast members will eventually want to join to the source tree that is the shortest route between the source and the group member.

You can configure a router to use a single RP for more than one group. The conditions specified by the access list determine which groups the RP can be used for. If no access list is configured, the RP is used for all groups.

A PIM router can use multiple RPs.

First-hop routers for multicast sources send register packets to all configured RPs. First-hop routers for multicast group members send join packets to one RP at a time. Once this router begins receiving multicast packets for the group, it will have joined one RP tree. Because the router does not want to receive multiple copies of the same packet, it joins only one RP tree.

Examples

The following example sets the PIM RP address to 198.92.37.33 for all multicast groups:

```
ip pim rp-address 198.92.37.33
```

The following example sets the PIM RP address to 147.106.6.22 for the multicast group 225.2.2.2 only:

```
access list 1 225.2.2.2 0.0.0.0
ip pim rp-address 147.106.6.22 1
```

Related Commands

A dagger (†) indicates that the command is documented in another chapter.

access-list (extended) †

access-list (standard) †

ip policy route-map

To identify a route map to use for policy routing on an interface, use the **ip policy route-map** interface configuration command. 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. Must match a *map-tag* specified by a **route-map** command.

Default

No policy routing occurs on the interface.

Command Mode

Interface configuration

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. 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.

Example

In the following example, packets with the destination IP address of 174.95.16.18 are sent to the router at IP address 174.21.3.20:

```
interface serial 0
ip policy route-map wethersfield
!
route-map wethersfield
match ip address 174.95.16.18
set ip next-hop 174.21.3.20
```

Related Commands

match ip address
match length
route-map
set default interface

```
set interface
set ip default next-hop
set ip next-hop
```

ip route

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

ip route *network [mask] {address | interface} [distance]*
no ip route

Syntax Description

<i>network</i>	IP address of the target network or subnet.
<i>mask</i>	(Optional) Network mask that lets you mask network and subnetwork bits.
<i>address</i>	IP address of the next hop that can be used to reach that network.
<i>interface</i>	Network interface to use.
<i>distance</i>	(Optional) An administrative distance.

Default

No static routes are established.

Command Mode

Global configuration

Usage Guidelines

A static route is appropriate when the router cannot dynamically build a route to the destination.

If you specify an administrative distance, you are flagging a static route that can be overridden by dynamic information. For example, IGRP-derived routes have a default administrative distance of 100. To have a static route that would be overridden by an IGRP 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 will be advertised via RIP, IGRP, and other dynamic routing protocols, regardless of whether **redistribute static** commands were specified for those routing protocols. This is because static routes that point to an interface are considered in the routing table to be connected and hence lose their static nature. However, if you define a static route to an interface that is not one of the networks defined in a **network** command, no dynamic routing protocols will advertise the route unless a **redistribute static** command is specified for these protocols.

Examples

In the following example, an administrative distance of 110 was chosen. In this case, packets for network 10.0.0.0 will be routed through to the router at 131.108.3.4 if dynamic information with administrative distance less than 110 is not available.

```
ip route 10.0.0.0 255.0.0.0 131.108.3.4 110
```

In the following example, packets for network 131.108.0.0 will be routed to the router at 131.108.6.6:

```
ip route 131.108.0.0 255.255.0.0 131.108.6.6
```

ip router isis

To configure an IS-IS routing process for IP on an interface, use the **ip router isis** interface configuration command. To disable IS-IS for IP, use the **no** form of this command.

ip router isis [*tag*]
no ip router isis [*tag*]

Syntax Description

tag (Optional) Defines a meaningful name for a routing process. If not specified, a null tag is assumed. It must be unique among all IP router processes for a given router. Use the same text for the argument *tag* as specified in the **router isis** global configuration command.

Default

No routing processes are specified.

Command Mode

Interface configuration

Example

The following example specifies IS-IS as an IP routing protocol for a process named Finance, and specifies that the Finance process will be routed on interfaces Ethernet 0 and serial 0:

```
router isis Finance
  interface Ethernet 0
    ip router isis Finance
  interface serial 0
    ip router isis Finance
```

Related Command

router isis

ip sd listen

To enable the router to listen to session directory advertisements, use the **ip sd listen** interface configuration command. To disable this feature, use the **no** form of this command.

```
ip sd listen
no ip sd listen
```

Syntax Description

This command has no arguments or keywords.

Default

Disabled

Command Mode

Interface configuration

Usage Guidelines

Session Directory Protocol is a multicast application for creating desktop conferencing sessions. It creates group addresses and allows the user to specify the scope of the group and whether audio, video, or whiteboard applications will be invoked when others open the session.

The **ip sd listen** command merely enables the router to listen to session directory advertisements. The router joins the default session directory group (group 224.2.127.255) on the interface. Use this command to get contact information.

Example

The following example enables the router to listen to session directory advertisements:

```
ip sd listen
```

Related Commands

```
clear ip sd
show ip sd
```

ip split-horizon

To enable the split-horizon mechanism, use the **ip split-horizon** interface configuration command. To disable the split-horizon mechanism, use the **no** form of this command.

ip split-horizon
no ip split-horizon

Syntax Description

This command has no arguments or keywords.

Default

Varies with media

Command Mode

Interface configuration

Usage Guidelines

For all interfaces except those for which either Frame Relay or SMDS encapsulation is enabled, the default condition for this command is **ip split-horizon**; in other words, the split horizon feature is active. If the interface configuration includes either the **encapsulation frame-relay** or **encapsulation smds** commands, then the default is for split horizon to be disabled. Split horizon is not disabled by default for interfaces using any of the X.25 encapsulations.

Note For networks that include links over X.25 PSNs, the **neighbor** router configuration command can be used to defeat the split horizon feature. You can as an alternative *explicitly* specify the **no ip split-horizon** command in your configuration. However, if you do so you *must* similarly disable split horizon for all routers in any relevant multicast groups on that network.

If split horizon has been disabled on an interface and you wish to enable it, use the **ip split-horizon** command to restore the split horizon mechanism.

Note In general, changing the state of the default for the **ip split-horizon** command is not recommended, unless you are certain that your application requires a change in order to properly advertise routes. If split horizon is disabled on a serial interface (and that interface is attached to a packet-switched network), you *must* disable split horizon for all routers in any relevant multicast groups on that network.

Example

The following simple example disables split horizon on a serial link. The serial link is connected to an X.25 network:

```
interface serial 0
encapsulation x25
no ip split-horizon
```

Related Commands

**ip split-horizon eigrp
neighbor**

ip split-horizon eigrp

To enable Enhanced IGRP split horizon, use the **ip split-horizon eigrp** interface configuration command. To disable split horizon, use the **no** form of this command.

```
ip split-horizon eigrp autonomous-system-number  
no ip split-horizon eigrp autonomous-system-number
```

Syntax Description

autonomous-system-number Autonomous system number.

Default

Enabled

Command Mode

Interface configuration

Usage Guidelines

For networks that include links over X.25 PSNs, you can use the **neighbor** router configuration command to defeat the split horizon feature. As an alternative, you can explicitly specify the **no ip split-horizon eigrp** command in your configuration. However, if you do so, you must similarly disable split horizon for all routers in any relevant multicast groups on that network.

In general, it is recommended that you not change the default state of split horizon unless you are certain that your application requires the change in order to properly advertise routes. Remember that if split horizon is disabled on a serial interface and that interface is attached to a packet-switched network, you must disable split horizon for all routers in any relevant multicast groups on that network.

Example

The following example disables split horizon on a serial link connected to an X.25 network:

```
interface serial 0  
encapsulation x25  
no ip split-horizon eigrp
```

Related Commands

ip split-horizon
neighbor

ip summary-address eigrp

To configure a summary aggregate address for a specified interface, use the **ip summary-address eigrp** interface configuration command. To disable a configuration, use the **no** form of this command.

```
ip summary-address eigrp autonomous-system-number address mask
no ip summary-address eigrp autonomous-system-number address mask
```

Syntax Description

<i>autonomous-system-number</i>	Autonomous system number.
<i>address</i>	IP summary aggregate address to apply to an interface.
<i>mask</i>	Subnet mask.

Default

No summary aggregate addresses are predefined.

Command Mode

Interface configuration

Usage Guidelines

Enhanced IGRP summary routes are given an administrative distance value of 5. You cannot configure this value.

Example

The following example sets the IP summary aggregate address for Ethernet interface 0:

```
interface ethernet 0
ip summary-address eigrp 109 192.1.0.0 255.255.0.0
```

Related Command

auto-summary

isis circuit-type

To configure the type of adjacency, use the **isis circuit-type** interface configuration command. To reset the circuit type to Level 1 and Level 2, use the **no** form of this command.

```
isis circuit-type {level-1 | level-1-2 | level-2-only}  
no isis circuit-type
```

Syntax Description

level-1	A Level 1 adjacency may be established if there is at least one area address in common between this system and its neighbors.
level-1-2	A Level 1 and Level 2 adjacency is established if the neighbor is also configured as level-1-2 and there is at least one area in common. If there is no area in common, a Level 2 adjacency is established. This is the default.
level-2-only	A Level 2 adjacency is established if and only if the neighbor is configured exclusively to be a Level 2 router.

Default

A Level 1 and Level 2 adjacency is established.

Command Mode

Interface configuration

Example

In the following example, a router is configured to require Level 1 adjacency if there is at least one area address in common between this system and its neighbors:

```
ip router isis  
interface serial 0  
isis circuit-type level-1
```

isis csnp-interval

To configure the IS-IS complete sequence number PDUs (CSNP) interval, use the **isis csnp-interval** interface configuration command. To restore the default value, use the **no** form of this command.

```
isis csnp-interval seconds {level-1 | level-2}
no isis csnp-interval {level-1 | level-2}
```

Syntax Description

<i>seconds</i>	Interval of time between transmission of CSNPs on multiaccess networks. This interval only applies for the designated router. The default is 10 seconds.
level-1	Configures the interval of time between transmission of CSNPs for Level 1 independently.
level-2	Configures the interval of time between transmission of CSNPs for Level 2 independently.

Default

10 seconds

Command Mode

Interface configuration

Usage Guidelines

This command only applies for the designated router (DR) for a specified interface. Only DRs send CSNP packets in order to maintain database synchronization. The CSNP interval can be configured independently for Level 1 and Level 2. This feature does not apply to serial point-to-point interfaces. It does apply to WAN connections if the WAN is viewed as a multiaccess meshed network.

Example

In the following example, serial interface 0 is configured for transmitting CSN PDUs every 5 seconds. The router is configured to act as a station router.

```
interface serial 0
isis csnp-interval 5 level-1
```

isis hello-interval

To specify the length of time between Hello packets that the router sends, use the **isis hello-interval** interface configuration command. To restore the default value, use the **no** form of this command.

```
isis hello-interval seconds {level-1 | level-2}  
no isis hello-interval {level-1 | level-2}
```

Syntax Description

<i>seconds</i>	Unsigned integer value. A value three times the Hello interval <i>seconds</i> is advertised as the <i>holdtime</i> in the Hello packets transmitted. It must be the same for all routers attached to a common network. With smaller Hello intervals, topological changes are detected faster, but there is more routing traffic. The default is 10 seconds.
level-1	Configures the Hello interval for Level 1 independently. Use this on X.25, SMDS, and Frame Relay multiaccess networks.
level-2	Configures the Hello interval for Level 2 independently. Use this on X.25, SMDS, and Frame Relay multiaccess networks.

Default

10 seconds

Command Mode

Interface configuration

Usage Guidelines

The Hello interval can be configured independently for Level 1 and Level 2, except on serial point-to-point interfaces. (Because there is only a single type of Hello packet sent on serial links, it is independent of Level 1 or Level 2.) The **level-1** and **level-2** keywords are used on X.25, SMDS, and Frame Relay multiaccess networks.

Example

In the following example, serial interface 0 is configured to advertise Hello packets every 5 seconds. The router is configured to act as a station router. This will cause more traffic than configuring a longer interval, but topological changes will be detected faster.

```
interface serial 0  
isis hello-interval 5 level-1
```

isis metric

To configure the metric for an interface, use the **isis metric** interface configuration command. To restore the default metric value, use the **no** form of this command.

```
isis metric default-metric [delay-metric [expense-metric [error-metric]]] {level-1 | level-2}  
no isis metric {level-1 | level-2}
```

Syntax Description

<i>default-metric</i>	Metric used for the redistributed route. The default metric is used as a value for the IS-IS metric. This is the value assigned when there is no QOS routing performed. Only this metric is supported by Cisco routers. You can configure this metric for Level 1 and/or Level 2 routing. The range is from 0 to 63. The default value is 10.
<i>delay-metric</i>	Not supported.
<i>expense-metric</i>	Not supported.
<i>error-metric</i>	Not supported.
level-1	Router acts as a station router (Level 1) only.
level-2	Router acts as an area router (Level 2) only.

Default

default-metric = 10

Command Mode

Interface configuration

Usage Guidelines

Specifying the **level-1** or **level-2** keywords resets the metric only for Level 1 or Level 2 routing, respectively.

Example

In the following example, serial interface 0 is configured for a default link-state metric cost of 15 for Level 1:

```
interface serial 0
isis metric 15 level-1
```

Related Commands

default-information
redistribute

isis password

To configure the authentication password for an interface, use the **isis password** interface configuration command. To disable authentication for IS-IS, use the **no** form of this command.

```
isis password password {level-1 | level-2}  
no isis password {level-1 | level-2}
```

Syntax Description

<i>password</i>	Authentication password you assign for an interface.
level-1	Configures the authentication password for Level 1 independently. For Level 1 routing, the router acts as a station router only.
level-2	Configures the authentication password for Level 2 independently. For Level 2 routing, the router acts as an area router only.

Default

Disabled

Command Mode

Interface configuration

Usage Guidelines

Different passwords can be assigned for different routing levels using the **level-1** and **level-2** keyword arguments.

Specifying the **level-1** or **level-2** keywords disables the password only for Level 1 or Level 2 routing, respectively. If no keyword is specified, the default is **level-1**.

Example

The following example configures a password for serial interface 0 at Level 1:

```
interface serial 0  
isis password frank level-1
```

isis priority

To configure the priority of designated routers, use the **isis priority** interface configuration command. To reset the default priority, use the **no** form of this command.

```
isis priority value {level-1 | level-2}  
no isis priority {level-1 | level-2}
```

Syntax Description

<i>value</i>	Sets the priority of a router and is a number from 0 to 127. The default value is 64.
level-1	Sets the priority of a router for Level 1 independently.
level-2	Sets the priority of a router for Level 2 independently.

Default

Priority of 64

Command Mode

Interface configuration

Usage Guidelines

Priorities can be configured for Level 1 and Level 2 independently. Specifying the **level-1** or **level-2** keywords resets priority only for Level 1 or Level 2 routing, respectively.

Example

The following example shows Level 1 routing given priority by setting the priority level to 50:

```
interface serial 0  
isis priority 50 level-1
```

isis retransmit-interval

To configure the time between retransmission of IS-IS link-state PDU (LSP) retransmission for point-to-point links, use the **isis retransmit-interval** interface configuration command. To restore the default value, use the **no** form of this command.

```
isis retransmit-interval seconds
no isis retransmit-interval seconds
```

Syntax Description

<i>seconds</i>	Time in seconds between retransmission of IS-IS LSP retransmissions. It is an integer that should be greater than the expected round-trip delay between any two routers on the attached network. The default is 5 seconds.
----------------	--

Default

5 seconds

Command Mode

Interface configuration

Usage Guidelines

The setting of the *seconds* argument should be conservative, or needless retransmission will result. The value should be larger for serial lines and virtual links.

Example

The following example configures serial interface 0 for retransmission of IS-IS LSP every 10 seconds for a large serial line:

```
interface serial 0
isis retransmit-interval 10
```

Related Commands

A dagger (†) indicates that the command is documented in another chapter.

encapsulation ppp †
frame-relay keepalive †
smds dxi †

is-type

To configure the IS-IS level at which the router operates, use the **is-type** router configuration command. To reset the default value, use the **no** form of this command.

```
is-type {level-1 | level-1-2 | level-2-only}  
no is-type {level-1 | level-1-2 | level-2-only}
```

Syntax Description

level-1	Router acts as a station router.
level-1-2	Router acts as both a station router and an area router.
level-2-only	Router acts as an area router only.

Default

Router acts as both a station router and an area router.

Command Mode

Router configuration

Example

The following example specifies an area router:

```
router isis  
is-type level-2-only
```

match as-path

To match a BGP autonomous system path access list, use the **match as-path** route-map configuration command. To remove a path list entry, the **no** form of this command.

match as-path *path-list-number*
no match as-path *path-list-number*

Syntax Description

path-list-number Autonomous system path access list. An integer from 1 through 199.

Default

No path lists are defined.

Command Mode

Route-map configuration

Usage Guidelines

The values set by the **match** and **set** commands override global values. For example, the weights assigned with the **match as-path** and **set weight** route-map commands override the weights assigned using the **neighbor weight** and **neighbor filter-list** commands.

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.

The implemented weight is based on the first matched autonomous system path.

Example

In the following example, the autonomous system path is set to match BGP autonomous system path access list 20:

```
route-map igrp2bgp
  match as-path 20
```

Related Commands

match community-list
match interface
match ip address
match ip next-hop
match ip route-source
match metric
match route-type
match tag
route-map
set as-path
set automatic-tag

set community
set level
set local-preference
set metric
set metric-type
set next-hop
set origin
set tag
set weight

match community-list

To match a BGP community, use the **match community-list** route-map configuration command. To remove the community list entry, use the **no** form of this command.

```
match community-list community-list-number [exact]
no match community-list community-list-number [exact]
```

Syntax Description

<i>community-list-number</i>	Community list number in the range from 1 through 99.
exact	(Optional) Indicates an exact match is required. All of the communities and only those communities in the community list must be present.

Default

No community list is defined.

Command Mode

Route-map configuration

Usage Guidelines

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.

Matching based on community list is one of the types of match clauses applicable to BGP.

Examples

In the following example, the routes that match community list 1 will have the weight set to 100. Any route that has community 109 will have the weight set to 100.

```
ip community-list 1 permit 109
!
route-map set_weight
match community-list 1
set weight 100
```

In the following example, the routes that match community list 1 will have the weight set to 200. Any route that has community 109 alone will have the weight set to 200.

```
ip community-list 1 permit 109
!
route-map set_weight
match community-list 1 exact
set weight 200
```

Related Commands

ip community-list
route-map
set weight

match interface

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

```
match interface type number...type number  
no match interface type number...type number
```

Syntax Description

<i>type</i>	Interface type.
<i>number</i>	Interface number.

Default

No match interfaces are defined.

Command Mode

Route-map configuration

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**. 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.

Example

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

match as-path
match community-list
match ip address
match ip next-hop
match ip route-source
match metric
match route-type
match tag
route-map
set as-path
set automatic-tag
set community
set level
set local-preference
set metric
set metric-type
set next-hop
set origin
set tag
set weight

match ip address

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

```
match ip address access-list-number...access-list-number  
no match ip address access-list-number...access-list-number
```

Syntax Description

<i>access-list-number</i>	Number of an access list. It can be an integer from 1 through 99. It can be an extended access list for policy routing.
---------------------------	---

Default

No access list numbers are specified.

Command Mode

Route-map configuration

Usage Guidelines

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**. 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 related **match** commands are listed in the section “Related Commands for Redistribution.” 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.

- **Policy Routing**

Another purpose of route maps is to enable policy routing. 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 to define the conditions for policy routing packets. Each **route-map** command has a list of **match** and **set** commands associated with it. The related **match** and **set** commands are listed in the section “Related Commands for Policy

Routing.” 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 and 80 will be distributed:

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

In the following policy routing example, packets that have addresses specified by access list numbers 6 and 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 for Redistribution

match as-path
match community-list
match interface
match ip next-hop
match ip route-source
match metric
match route-type
match tag
route-map
set as-path
set automatic-tag
set community
set level
set local-preference
set metric
set metric-type
set next-hop
set origin
set tag
set weight

Related Commands for Policy Routing

ip policy route-map
match length
route-map
set default interface
set interface
set ip default next-hop
set ip next-hop

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** route-map configuration command. To remove the next-hop entry, use the **no** form of this command.

```
match ip next-hop access-list-number...access-list-number
no match ip next-hop access-list-number...access-list-number
```

Syntax Description

<i>access-list-number</i>	Number of an access list. It can be an integer from 1 through 99.
---------------------------	---

Default

Routes are distributed freely, without being required to match a next-hop address.

Command Mode

Route-map configuration

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**. 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.

Example

In the following example, 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

match as-path
match community-list
match interface

```
match ip address
match ip route-source
match metric
match route-type
match tag
route-map
set as-path
set automatic-tag
set community
set level
set local-preference
set metric
set metric-type
set next-hop
set origin
set tag
set weight
```

match ip route-source

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

```
match ip route-source access-list-number...access-list-number  
no match ip route-source access-list-number...access-list-number
```

Syntax Description

access-list-number Number of an access list. It can be an integer from 1 through 99.

Default

No filtering on route source.

Command Mode

Route-map configuration

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**. 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 second route-map section with an explicit match specified.

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

Example

In the following example, routes that have been advertised by routers at the addresses specified by access lists 5 and 80 will be distributed:

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

Related Commands

match as-path
match community-list
match interface
match ip address
match ip next-hop
match metric
match route-type
match tag
route-map
set as-path
set automatic-tag
set community
set level
set local-preference
set metric
set metric-type
set next-hop
set origin
set tag
set weight

match length

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

```
match length min max
no match length min max
```

Syntax Description

min Minimum Level 3 length of the packet, inclusive, allowed for a match.
Range is 0 through 0x7FFFFFFF.

max Maximum Level 3 length of the packet, inclusive, allowed for a match.
Range is 0 through 0x7FFFFFFF.

Default

No policy routing on the length of a packet.

Command Mode

Route-map configuration

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.

Example

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

ip policy route-map
match ip address
route-map
set default interface
set interface
set ip default next-hop
set ip next-hop

match metric

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

```
match metric metric-value  
no match metric metric-value
```

Syntax Description

<i>metric-value</i>	Route metric, which can be an IGRP five-part metric. It is a metric value from 0 through 4294967295.
---------------------	--

Default

No filtering on a metric value.

Command Mode

Route-map configuration

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**. 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 second route-map section with an explicit match specified.

Example

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

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

Related Commands

match as-path
match community-list
match interface
match ip address

```
match ip next-hop
match ip route-source
match route-type
match tag
route-map
set as-path
set automatic-tag
set community
set level
set local-preference
set metric
set metric-type
set next-hop
set origin
set tag
set weight
```

match route-type

To redistribute routes of the specified type, use the **match route-type** route-map configuration command. 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 BGP routes.
internal	OSPF intra-area and interarea routes or enhanced IGRP internal routes.
external [type-1 type-2]	OSPF external routes, or enhanced IGRP external routes. For OSPF, external type-1 matches only type 1 external routes and external type-2 matches only type 2 external routes.
level-1	IS-IS Level 1 routes.
level-2	IS-IS Level 2 routes.

Default

Disabled

Command Mode

Route-map configuration

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**. 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 second route-map section with an explicit match specified.

Example

In the following example, internal routes will be redistributed:

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

Related Commands

match as-path
match community-list
match interface
match ip address
match ip next-hop
match ip route-source
match metric
match tag
route-map
set as-path
set automatic-tag
set community
set level
set local-preference
set metric
set metric-type
set next-hop
set origin
set tag
set weight

match tag

To redistribute routes in the routing table that match the specified tags, use the **match tag** route-map configuration command. 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

<i>tag-value</i>	List of one or more route tag values. Each can be an integer from 0 through 4294967295.
------------------	---

Default

No match tag values are defined.

Command Mode

Route-map configuration

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**. 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 second route-map section with an explicit match specified.

Example

In the following example, routes stored in the routing table with tag 5 will be redistributed:

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

Related Commands

match as-path
match community-list
match interface
match ip address

```
match ip next-hop
match ip route-source
match metric
match route-type
route-map
set as-path
set automatic-tag
set community
set level
set local-preference
set metric
set metric-type
set next-hop
set origin
set tag
set weight
```

mbranch

To trace a branch of a multicast tree for a specific group, use the **mbranch** EXEC command.

```
mbranch {group-address | group-name} branch [ttl]
```

Syntax Description

<i>group-address</i>	Address of the multicast group. This is a multicast IP address in four-part dotted notation.
<i>group-name</i>	Name of the multicast group, as defined in the DNS hosts table or with the ip host command.
<i>branch</i>	Address or name of a router that is on the tree branch. The address is a unicast IP address in four-part dotted notation.
<i>ttl</i>	(Optional) Time-to-live value, in hops, that is used in trace request packets sent to the branch router. The default value is 30.

Command Mode

EXEC

Usage Guidelines

The **mbranch** command sends multicast IGMP trace request packets to the specified branch router. It displays information about the branch starting with the local (requesting) router and ending with the branch router. This is considered to be the forward direction.

The information returned shows how a multicast packet sourced by this router will be forwarded by each router on the path to the router with the branch address.

The router with the address *branch-address* is the only router that responds to the trace request packets. The response is unicast to the source.

It is important to specify a value for the *ttl* argument if you are tracing through a router on which a multicast threshold has been set with the **ip multicast ttl-threshold** interface configuration command.

Sample Display

The following is sample output from the **mbranch** command. This trace is between the same routers as shown in the example for the **mbranch** command. Note the order of responses. Also note that the outgoing interface list is the same.

```
PIM2# mbranch 224.0.255.2 198.92.118.2
Type escape sequence to abort.
Tracing route to group CBONE-WB (224.0.255.2) to 198.92.118.2
Response from 10.17.118.10, 76 msec
 1 PIM9 (10.1.22.9) <- PIM2 (10.1.37.2)
    Interface list: 131.108.62.0/24 131.108.22.0/24 10.7.0.0/16
  2 PIM-CR (131.108.62.18) <- PIM9 (131.108.62.52)
    Interface list: 131.108.20.0/24 131.108.53.0/24 131.108.50.0/24
                  10.16.0.0/16 10.17.0.0/16
```

```
3 10.17.118.10 <- 10.17.20.31
  Interface list: 198.92.118.0/26 198.92.118.192/26
```

The **mbranch** command is interactive if you specify only the word **mbranch**. The following output shows sample responses to the system prompts:

```
Router# mbranch
Target IP group address or name:224.0.255.1
Target IP router address or name:sj-eng-f2
Ttl [30]:10
Source address or name:<CR>
Interface:ethernet0
Type escape sequence to abort.
Tracing route to group cbone-audio.cisco.com (224.0.255.1) to 171.69.4.139
Response from sj-eng-f2.cisco.com (171.69.4.139), 4 msec
  1 sj-eng-cc2.cisco.com (171.69.121.2)<- 0.0.0.0
    Interface list: 171.69.4.0/24
  2 sj-eng-f2.cisco.com (171.69.4.139)<- sj-eng-cc2.cisco.com (171.69.4.135)
    Interface list: 171.69.60.128/26
```

Table 19-3 describes the fields shown in the first display.

Table 19-3 Mbranch Field Descriptions

Field	Description
Response from 10.17.118.10	Address of the router from which the response to the trace request packets came. This is a different interface on the router to which you sent the packet.
76 msec	How long it took to receive the response.
1	Order number of routers in the trace path. In this example, the request went through 3 routers to reach the router that responded to the request.
PIM9 (10.1.22.9) <- PIM2 (10.1.37.2)	Route of the trace request. In this example, the request went from the router PIM2 to the router PIM9 (PIM2 is considered to be PIM9's RPF neighbor), then from PIM9 to PIM-CR, and finally to the router at 10.17.118.10.
Interface list: 131.108.62.0/24 131.108.22.0/24 10.7.0.0/16	Interfaces out which a multicast packet forwarded by the router listed on the right side of the previous line (here, PIM2) will be forwarded. In this example, you interpret this line as follows: When the trace packet reached PIM9, it was replicated three times and one copy was sent out each of the three interfaces listed (131.108.62.0, 131.108.22.0, and 10.7.0.0). The interface list shows the subnet number and the mask rather than the interface name. This allows you to more easily figure out the packet's path because you can connect all like-numbered subnets together as a tree in order to detect loops. The source of the multicast packet is always the address of the router that started the mbranch (in this case, 10.1.37.2). The list does not include interfaces that failed access list conditions or TTL threshold criteria.

Related Commands

ip multicast ttl-threshold
mrbranch

metric holddown

To keep new IGRP routing information from being used for a certain period of time, use the **metric holddown** router configuration command. To disable this feature, use the **no** form of this command.

metric holddown
no metric holddown

Syntax Description

This command has no arguments or keywords.

Default

Disabled

Command Mode

Router configuration

Usage Guidelines

Holddown keeps new routing information from being used for a certain period of time. This can prevent routing loops caused by slow convergence. It is sometimes advantageous to disable holddown to increase the network's ability to quickly respond to topology changes; this command provides this function.

Use the **metric holddown** command if other routers within the IGRP autonomous system are not configured with **no metric holddown**. If all routers are not configured the same way, you increase the possibility of routing loops.

Example

The following example disables metric holddown:

```
router igrp 15
network 131.108.0.0
network 192.31.7.0
no metric holddown
```

Related Commands

metric maximum-hops

metric weights

timers basic (EGP, RIP, IGRP)

metric maximum-hops

To have the IP routing software to advertise as unreachable those routes with a hop count higher than is specified by the command (IGRP only), use the **metric maximum-hops** router configuration command. To reset the value to the default, use the **no** form of this command.

metric maximum-hops *hops*
no metric maximum-hops *hops*

Syntax Description

hops Maximum hop count (in decimal). The default value is 100 hops; the maximum number of hops that can be specified is 255.

Default

100 hops

Command Mode

Router configuration

Usage Guidelines

This command provides a safety mechanism that breaks any potential *count-to-infinity* problems. It causes the IP routing software to advertise as unreachable routes with a hop count greater than the value assigned to the *hops* argument.

Example

In the following example, a router in autonomous system 71 attached to network 15.0.0.0 wants a maximum hop count of 200, doubling the default. The network administrators decided to do this because they have a complex WAN that can generate a large hop count under normal (nonlooping) operations.

```
router igrp 71
network 15.0.0.0
metric maximum-hops 200
```

Related Commands

metric holddown
metric weights

metric weights

To allow the tuning of the IGRP or Enhanced IGRP metric calculations, use the **metric weights** router configuration command. To reset the values to their defaults, use the **no** form of this command.

```
metric weights tos k1 k2 k3 k4 k5  
no metric weights
```

Syntax Description

<i>tos</i>	Type of service. Currently, it must always be zero.
<i>k1</i> – <i>k5</i>	Constants that convert an IGRP or enhanced IGRP metric vector into a scalar quantity.

Default

```
tos: 0  
k1: 1  
k2: 0  
k3: 1  
k4: 0  
k5: 0
```

Command Mode

Router configuration

Usage Guidelines

Use this command to alter the default behavior of IGRP routing and metric computation and allow the tuning of the IGRP metric calculation for a particular type of service (TOS).

If *k5* equals 0, the composite IGRP or enhanced IGRP metric is computed according to the following formula:

```
metric = [k1 * bandwidth + (k2 * bandwidth)/(256 - load) + k3 * delay]
```

If *k5* does not equal zero, an additional operation is done:

```
metric = metric * [k5 / (reliability + k4)]
```

Bandwidth is inverse minimum bandwidth of the path in bits per second scaled by a factor of 2.56×10^{12} . The range is from a 1200-bps line to 10 terabits per second.

Delay is in units of 10 microseconds. This gives a range of 10 microseconds to 168 seconds. A delay of all ones indicates that the network is unreachable.

The delay parameter is stored in a 32-bit field, in increments of 39.1 nanoseconds. This gives a range of 1 (39.1 nanoseconds) to hexadecimal FFFFFFFF (decimal 4,294,967,040 nanoseconds). A delay of all ones (that is, a delay of hexadecimal FFFFFFFF) indicates that the network is unreachable.

Table 19-4 lists the default values used for several common media.

Table 19-4 Bandwidth Values by Media Type

Media Type	Delay	Bandwidth
Satellite	5120 (2 seconds)	5120 (500 Mbits)
Ethernet	25600 (1 ms)	256000 (10 Mbits)
1.544 Mbps	512000 (20,000 ms)	1,657,856 bits
64 kbps	512000 (20,000 ms)	40,000,000 bits
56 kbps	512000 (20,000 ms)	45,714,176 bits
10 kbps	512000 (20,000 ms)	256,000,000 bits
1 kbps	512000 (20,000 ms)	2,560,000,000 bits

Reliability is given as a fraction of 255. That is, 255 is 100 percent reliability or a perfectly stable link.

Load is given as a fraction of 255. A load of 255 indicates a completely saturated link.

Example

The following example sets the metric weights to slightly different values than the defaults:

```
router igrp 109
network 131.108.0.0
metric weights 0 2 0 2 0 0
```

Related Commands

A dagger (†) indicates that the command is documented in another chapter.

bandwidth †
delay †
metric holddown
metric maximum-hops

mrbranch

To trace a branch of a multicast tree for a group in the reverse direction, use the **mrbranch** EXEC command.

mrbranch {*group-address* | *group-name*} *branch-address* [*ttl*]

Syntax Description

<i>group-address</i>	Address of the multicast group. This is a multicast IP address in four-part dotted notation.
<i>group-name</i>	Name of the multicast group, as defined in the DNS hosts table or with the ip host command.
<i>branch-address</i>	Address of a router on the tree branch. This is a unicast IP address in four-part dotted notation.
<i>ttl</i>	(Optional) Time-to-live value, in hops, that is used in trace request packets sent to the branch router. The default value is 30.

Command Mode

EXEC

Usage Guidelines

The **mrbranch** command sends trace request packets to the specified branch router. Queries are sent recursively to all the routers in the branch. This command displays information about the branch starting with the router farthest away and working towards the requesting router. This is considered to be the reverse direction.

The information returned shows how a multicast packet sourced by this router will be forwarded by each router along the branch.

The router with the address *branch-address* responds to the trace request packets. The requesting router then sends a query to the router that is the first router's RPF neighbor. Both the request and response packets have unicast addresses.

The number of packets generated by this command is two times the number of routers between the source router and the specified branch router.

Sample Output

The following is sample output from the **mrbranch** command. This example is between the same router as shown in the **mbranch** command. Note the order of the responses. Also note that the outgoing interface list is the same.

```
PIM2# mrbranch 224.0.255.2 10.17.118.10

Type escape sequence to abort.
Tracing route to group CBONE-WB (224.0.255.2) from 10.17.118.10

Response from 10.17.118.10, 68 msec
 1 10.17.118.10 <- 10.17.20.31
    Interface list: 198.92.118.0/26 198.92.118.192/26
    Response from PIM-CR (131.108.62.18), 12 msec
```

```

1 PIM-CR (131.108.62.18) <- PIM9 (131.108.62.52)
  Interface list: 131.108.20.0/24 131.108.53.0/24 131.108.50.0/24
                  10.16.0.0/16 10.17.0.0/16
Response from PIM9 (131.108.62.52), 8 msec
1 PIM9 (131.108.62.52) <- PIM2 (10.1.37.2)
  Interface list: 131.108.22.0/24 131.108.62.0/24 10.7.0.0/16

```

The **mrbranch** command is interactive if you specify only the word **mrbranch**. The following output shows sample responses to the system prompts:

```

Router# mrbranch
Target IP group address or name:224.0.255.1
Target IP router address or name:sj-eng-f2
Ttl [30]:10
Source address or name:<CR>
Interface:ethernet0
Type escape sequence to abort.
Tracing route to group cbone-audio.cisco.com (224.0.255.1) to 171.69.4.139
Response from sj-eng-f2.cisco.com (171.69.4.139), 4 msec
1 sj-eng-f2.cisco.com (171.69.4.139)<- sj-eng-cc2.cisco.com (171.69.4.135)
  Interface list: 171.69.60.128/26
Response from sj-eng-f2.cisco.com (171.69.121.2), 4 msec
1 sj-eng-cc2.cisco.com (171.69.121.2)<- 0.0.0.0
  Interface list: 171.69.4.0/24

```

Table 19-5 describes the fields shown in the display.

Table 19-5 Mrbranch Field Descriptions

Field	Description
Tracing route to group CBONE-WB (224.0.255.2) from 10.17.118.10	Route that is being traced.
68 msec	How long it took to receive the response.
Response from 10.17.118.10	Address of the router from which the response to the trace request packets came.
1	Order number of routers in the trace path.
10.17.118.10 <- 10.17.20.31	RPF (reverse path forwarding) neighbor information. The first response in this example indicates that a multicast packet sent from the router PIM2 will be received on interface 10.17.118.10. This multicast packet should have been forwarded from 10.17.20.31 because that is the address that this router would use as the next-hop router (found in the IP routing table) to send a unicast packet back to the original source (PIM2) of the multicast packet.
Interface list: 198.92.118.0/26 198.92.118.192/26	Interfaces out which a multicast packet from the router listed on the right side of the previous line (here, for the group 224.0.255.2 that had been forwarded by 10.17.20.31) will be forwarded. The list does not include interfaces that failed access list conditions or TTL threshold criteria.

Related Commands

mbranch
show ip mroute

neighbor (EGP, IGRP, RIP)

To define a neighboring router with which to exchange routing information, use this form of the **neighbor** router configuration command. To remove an entry, use the **no** form of this command.

neighbor *ip-address*
no neighbor *ip-address*

Syntax Description

ip-address IP address of a peer router with which routing information will be exchanged.

Default

No neighboring routers are defined.

Command Mode

Router configuration

Usage Guidelines

For exterior routing protocol EGP, this command specifies routing peers. For normally broadcast protocols such as IGRP or RIP, this command permits the point-to-point (nonbroadcast) exchange of routing information. When used in combination with the **passive-interface** router configuration command, routing information can be exchanged between a subset of routers on a LAN.

Multiple **neighbor** commands can be used to specify additional neighbors or peers.

OSPF has its own version of the **neighbor** command. See the **neighbor (OSPF)** command page in this chapter.

Examples

The following example establishes an EGP neighbor:

```
autonomous-system 109
router egp 110
neighbor 131.108.1.1
```

In the following example, IGRP updates are sent to all interfaces on network 131.108.0.0 except interface Ethernet 1. However, in this case a **neighbor** router configuration command is included. This command permits the sending of routing updates to specific neighbors. One copy of the routing update is generated per neighbor.

```
router igrp 109
network 131.108.0.0
passive-interface ethernet 1
neighbor 131.108.20.4
```

Related Command

passive-interface

neighbor (OSPF)

To configure OSPF routers interconnecting to nonbroadcast networks, use this form of the **neighbor** router configuration command. To remove a configuration, use the **no** form of this command.

```
neighbor ip-address [priority number] [poll-interval seconds]
no neighbor ip-address [priority number] [poll-interval seconds]
```

Syntax Description

<i>ip-address</i>	Interface IP address of the neighbor.
<i>number</i>	(Optional) 8-bit number indicating the router priority value of the nonbroadcast neighbor associated with the IP address specified. The default is 0.
<i>seconds</i>	(Optional) Unsigned integer value reflecting the poll interval. RFC 1247 recommends that this value be much larger than the Hello interval. The default is 2 minutes (120 seconds).

Default

No configuration is specified.

Command Mode

Router configuration

Usage Guidelines

X.25 and Frame Relay provide an optional broadcast capability that can be configured in the map to allow OSPF to run as a broadcast network. At the OSPF level you can configure the router as a broadcast network. See the **x25 map** and **frame-relay map** commands in “X.25 Commands” and “Frame Relay Commands” chapters, respectively, for more detail.

One neighbor entry must be included in the router’s configuration for each known nonbroadcast network neighbor. The neighbor address has to be on the primary address of the interface.

If a neighboring router has become inactive (Hello packets have not been seen for the Router Dead Interval period), it may still be necessary to send Hello packets to the dead neighbor. These Hello packets will be sent at a reduced rate called *Poll Interval*.

When the router first starts up, it sends only Hello packets to those routers with non-zero priority, that is, routers which are eligible to become designated routers (DR) and backup designated routers (BDR). After DR and BDR are selected, DR and BDR will then start sending Hello packets to all neighbors in order to form adjacencies.

Example

The following example declares a router at address 131.108.3.4 on a nonbroadcast network, with a priority of 1 and a poll-interval of 180:

```
router ospf
neighbor 131.108.3.4 priority 1 poll-interval 180
```

Related Command

ip ospf priority

neighbor advertisement-interval

To set the minimum interval between the sending of BGP routing updates, use the **neighbor advertisement-interval** router configuration command. To remove an entry, use the **no** form of this command.

```
neighbor {ip-address | peer-group-name} advertisement-interval seconds
no neighbor {ip-address | peer-group-name} advertisement-interval seconds
```

Syntax Description

<i>ip-address</i>	Neighbor's IP address.
<i>peer-group-name</i>	Name of a BGP peer group.
<i>seconds</i>	Time in seconds. Integer from 0 through 600.

Default

30 seconds for external peers and 5 seconds for internal peers.

Command Mode

Router configuration

Usage Guidelines

If you specify a BGP peer group by using the *peer-group-name* argument, all of the members of the peer group will inherit the characteristic configured with this command.

Example

In the following example, the minimum time between sending BGP routing updates is set to 10 seconds:

```
router bgp 5
neighbor 4.4.4.4 advertisement-interval 10
```

Related Command

neighbor peer-group (creating)

neighbor any

To control how neighbor entries are added to the routing table for both EGP and BGP, use the **neighbor any** router configuration command. To remove a configuration, use the **no** form of this command.

```
neighbor any [access-list-number]  
no neighbor any [access-list-number]
```

Syntax Description

<i>access-list-number</i>	(Optional) Access list number the neighbor must be accepted by to be allowed to peer with the EGP or BGP process. If no list is specified, any neighbor will be allowed to peer with the router.
---------------------------	--

Default

No configuration is specified.

Command Mode

Router configuration

Example

In the following example, only neighbors permitted by access list 1 are allowed to peer with the local router:

```
access-list 1 permit 10.0.0.0 0.255.255.255
! global access list assignment
router egp 0
neighbor any 1
```

Related Commands

A dagger (†) indicates that the command is documented in another chapter.

access-list (standard) [†]
neighbor any third-party
router egp 0

neighbor any third-party

To configure an EGP process that determines which neighbors are treated as the next hop in EGP advertisements, use the **neighbor any third-party** router configuration command. To remove a configuration, use the **no** form of this command.

neighbor any third-party *ip-address* [**internal** | **external**]
no neighbor any third-party *ip-address* [**internal** | **external**]

Syntax Description

<i>ip-address</i>	IP address of the third-party router that is to be the next hop in EGP advertisements.
internal	(Optional) Indicates that the third-party router should be listed in the internal section of the EGP update.
external	(Optional) Indicates that the third-party router should be listed in the external section of the EGP update.

Default

No EGP process is configured.

Command Mode

Router configuration

Example

The following example specifies the particular neighbors that an EGP process will view as peers:

```
access-list 2 permit 10.0.0.0 0.255.255.255
! global access list assignment
router egp 0
neighbor any 2
neighbor any third-party 10.1.1.1
```

Related Commands

neighbor any
router egp 0

neighbor configure-neighbors

To have the router treat temporary neighbors that have been accepted by a template as if they had been configured manually, use the **neighbor configure-neighbors** router configuration command. To restore the default, use the **no** form of this command.

neighbor *template-name* configure-neighbors
no neighbor *template-name* configure-neighbors

Syntax Description

template-name User-selectable designation that identifies a particular template. This can be an arbitrary word.

Default

New neighbors are treated as temporary.

Command Mode

Router configuration

Usage Guidelines

Under normal circumstances, neighbors that are allowed to connect to the router because you had configured a template are treated as temporary. When a temporary neighbor disconnects, the local router will not try to actively reestablish a connection with it. In addition, information about temporary neighbors will not show up in the router configuration (**write terminal**).

When **configure-neighbors** is enabled on a particular template, any neighbor accepted by that template will be treated as if it had been manually configured. These neighbors will show up in **write terminal** displays and will be written to the nonvolatile configuration if a **write memory** command is issued.

Example

In the following example, any BGP speaker matching access list 7 can connect to the router and exchange information. Any neighbor that connects will be treated as if it had been manually configured.

```
access-list 7 permit 168.89.3.0 0.0.0.255
neighbor internal-ethernet neighbor-list 7
neighbor internal-ethernet configure-neighbors
```

Related Command

neighbor neighbor-list

neighbor default-originate

To allow a BGP speaker (the local router) to send the default route 0.0.0.0 to a neighbor for use as a default route, use the **neighbor default-originate** router configuration command. To remove the default route, use the **no** form of this command.

```
neighbor {ip-address | peer-group-name} default-originate [route-map map-name]
no neighbor {ip-address | peer-group-name} default-originate [route-map map-name]
```

Syntax Description

<i>ip-address</i>	Neighbor's IP address.
<i>peer-group-name</i>	Name of a BGP peer group.
<i>map-name</i>	(Optional) Name of the route map. The route map allows route 0.0.0.0 to be injected conditionally.

Default

No default route is sent to the neighbor.

Command Mode

Router configuration

Usage Guidelines

This command does not require the presence of 0.0.0.0 in the local router. When used with a route map, the default route 0.0.0.0 is injected if the route map contains a **match ip address** clause and there is a route that matches the IP access list exactly. The route map can contain other match clauses also.

Examples

In the following example, the local router injects route 0.0.0.0 to the neighbor 160.89.2.3 unconditionally:

```
router bgp 109
network 160.89.0.0
neighbor 160.89.2.3 remote-as 200
neighbor 160.89.2.3 default-originate
```

In the following example, the local router injects route 0.0.0.0 to the neighbor 160.89.2.3 only if there is a route to 198.92.68.0:

```
router bgp 109
network 160.89.0.0
neighbor 160.89.2.3 remote-as 200
neighbor 160.89.2.3 default-originate route-map default-map
!
route-map default-map 10 permit
match ip address 1
!
access-list 1 permit 198.92.68.0
```

neighbor distribute-list

To distribute BGP neighbor information as specified in an access list, use the **neighbor distribute-list** router configuration command. To remove an entry, use the **no** form of this command.

```
neighbor {ip-address | peer-group-name} distribute-list access-list-number {in | out}  
no neighbor {ip-address | peer-group-name} distribute-list access-list-number {in | out}
```

Syntax Description

<i>ip-address</i>	Neighbor's IP address.
<i>peer-group-name</i>	Name of a BGP peer group.
<i>access-list-number</i>	Predefined access list number. Only standard access lists can be used with this command.
in	Access list is applied to incoming advertisements to that neighbor.
out	Access list is applied to outgoing advertisements from that neighbor.

Default

No BGP neighbor is specified.

Command Mode

Router configuration

Usage Guidelines

Using distribute lists is one of two ways to filter BGP advertisements. The other way is to use AS-path filters, as with the **ip as-path access-list** global configuration command and the **neighbor filter-list** command.

If you specify a BGP peer group by using the *peer-group-name* argument, all of the members of the peer group will inherit the characteristic configured with this command. Specifying the command with an IP address will override the value inherited from the peer group.

Example

The following example applies list 39 to incoming advertisements to neighbor 120.23.4.1:

```
router bgp 109  
network 131.108.0.0  
neighbor 120.23.4.1 distribute-list 39 in
```

Related Commands

ip as-path access-list
neighbor filter-list
neighbor peer-group (creating)

neighbor ebgp-multipath

To accept and attempt BGP connections to external peers residing on networks that are not directly connected, use the **neighbor ebgp-multipath** router configuration command. To return to the default, use the **no** form of this command.

```
neighbor {ip-address | peer-group-name} ebgp-multipath [ttl]
no neighbor {ip-address | peer-group-name} ebgp-multipath
```

Syntax Description

<i>ip-address</i>	IP address of the BGP-speaking neighbor.
<i>peer-group-name</i>	Name of a BGP peer group.
<i>ttl</i>	Time-to-live in the range 1 to 255 hops.

Default

Only directly connected neighbors are allowed.

Command Mode

Router configuration

Usage Guidelines

This feature should only be used under the guidance of technical support staff.

If you specify a BGP peer group by using the *peer-group-name* argument, all of the members of the peer group will inherit the characteristic configured with this command.

Example

The following example allows connections to or from neighbor 131.108.1.1, which resides on a network that is not directly connected:

```
router bgp 109
neighbor 131.108.1.1 ebgp-multipath
```

Related Command

neighbor peer-group (creating)

neighbor filter-list

To set up a BGP filter, use the **neighbor filter-list** router configuration command. To disable this function, use the **no** form of this command.

```
neighbor {ip-address | peer-group-name} filter-list access-list-number {in | out |  
    weight weight}  
no neighbor {ip-address | peer-group-name} filter-list access-list-number {in | out |  
    weight weight}
```

Syntax Description

<i>ip-address</i>	IP address of the neighbor.
<i>peer-group-name</i>	Name of a BGP peer group.
<i>access-list-number</i>	Number of an autonomous system path access list. You define this access list with the ip as-path access-list command.
in	Access list to incoming routes.
out	Access list to outgoing routes.
weight <i>weight</i>	Assigns a relative importance to incoming routes matching autonomous system paths. Acceptable values are 0 to 65535.

Default

Disabled

Command Mode

Router configuration

Usage Guidelines

This command establishes filters on both inbound and outbound BGP routes. Any number of weight filters are allowed on a per-neighbor basis, but only one in or out filter is allowed. The weight of a route affects BGP's route-selection rules.

The implemented weight is based on the first matched autonomous system path. Weights indicated when an autonomous system path is matched override the weights assigned by global **neighbor** commands. In other words, the weights assigned with the **match as-path** and **set weight** route-map commands override the weights assigned using the **neighbor weight** and **neighbor filter-list** commands.

See the “Regular Expressions” appendix for information on forming regular expressions.

If you specify a BGP peer group by using the *peer-group-name* argument, all of the members of the peer group will inherit the characteristic configured with this command. Specifying the command with an IP address will override the value inherited from the peer group.

Example

In the following example, the BGP neighbor with IP address 128.125.1.1 is not sent advertisements about any path through or from the adjacent autonomous system 123:

```
ip as-path access-list 1 deny _123_
ip as-path access-list 1 deny ^123$ |  
  
router bgp 109
network 131.108.0.0
neighbor 129.140.6.6 remote-as 123
neighbor 128.125.1.1 remote-as 47
neighbor 128.125.1.1 filter-list 1 out
```

Related Commands

ip as-path access-list
neighbor distribute-list
neighbor peer-group (creating)
neighbor weight

neighbor neighbor-list

To configure BGP to support anonymous neighbor peers by configuring a neighbor template, use the **neighbor neighbor-list** router configuration command. To delete a template, use the **no** form of this command.

neighbor *template-name* neighbor-list *access-list-number*
no neighbor *template-name* neighbor-list

Syntax Description

<i>template-name</i>	User-selectable designation that identifies a particular template (an arbitrary word).
<i>access-list-number</i>	Number of an access list. It can be a number in the range 1 through 99.

Default

No configuration is defined.

Command Mode

Router configuration

Usage Guidelines

To specify a group of anonymous neighbors, configure a neighbor template rather than specifically configure each neighbor. The template allows you to specify an IP access list which defines remote systems that can establish a BGP connection to the router. External BGP peers must be on a directly connected Ethernet unless they are overridden by the **neighbor ebgp-multihop** command.

Once you specify a template, you configure the template as if it were a regular neighbor entry, such as setting the protocol version or filter lists, so that anonymous neighbors accepted by the template will receive the settings of the template.

These neighbors accepted by the template appear in the **show ip bgp summary** and **show ip bgp neighbors** displays, although they do not appear in the router configuration. When the session is disconnected, all knowledge about the neighbor is discarded and the router will not attempt to actively reestablish a connection.

You can use the **neighbor configure-neighbors** command to request that the router treat peers learned through a template as if they were manually configured neighbors. These peers will then show up in **write terminal** displays and can be stored as part of the nonvolatile configuration.

The **no neighbor neighbor-list** command deletes the template and cause any temporary neighbors accepted by the template to be shut down and removed.

Examples

In the following example, any BGP speaker from 168.89.3.0 can connect to the router and exchange information:

```
access-list 7 permit 168.89.3.0 0.0.0.255
neighbor internal-ethernet neighbor-list 7
neighbor internal-ethernet configure-neighbors
```

In the following example, any BGP speaker in the connected internet can establish a BGP connection to the local router, and the local router will send them routing information. However, the **distribute-list** clause instructs the local router to ignore all information these remote BGP speakers send to it.

```
access-list 9 permit 0.0.0.0 255.255.255.255
access-list 10 deny 0.0.0.0 255.255.255.255
neighbor route-server-peers neighbor-list 9
neighbor route-server-peers distribute-list 10 in
```

Related Commands

A dagger (†) indicates that the command is documented in another chapter.

access-list (standard) †

neighbor configure-neighbors

neighbor ebgp-multipath

neighbor next-hop-self

To disable next-hop processing of BGP updates on the router, use the **neighbor next-hop-self** router configuration command. To disable this feature, use the **no** form of this command.

```
neighbor {ip-address | peer-group-name} next-hop-self  
no neighbor {ip-address /| peer-group-name} next-hop-self
```

Syntax Description

ip-address IP address of the BGP-speaking neighbor.

peer-group-name Name of a BGP peer group.

Default

Disabled

Command Mode

Router configuration

Usage Guidelines

This command is useful in nonmeshed networks such as Frame Relay or X.25 where BGP neighbors may not have direct access to all other neighbors on the same IP subnet.

If you specify a BGP peer group by using the *peer-group-name* argument, all of the members of the peer group will inherit the characteristic configured with this command. Specifying the command with an IP address will override the value inherited from the peer group.

Example

The following example forces all updates destined for 131.108.1.1 to advertise this router as the next hop:

```
router bgp 109  
neighbor 131.108.1.1 next-hop-self
```

Related Command

neighbor peer-group (creating)

neighbor password

To enable MD5 authentication on a TCP connection between two BGP peers, use the **neighbor password** router configuration command. To disable this feature, use the **no** form of this command.

neighbor {ip-address | peer-group-name} password string
no neighbor {ip-address | peer-group-name} password

Syntax Description

ip-address IP address of the BGP-speaking neighbor.

peer-group-name Name of a BGP peer group.

string Case-sensitive password of up to 80 characters. The first character cannot be a number. The string can contain any alphanumeric characters, including spaces. You cannot specify a password in the format *number-space-anything*. The space after the number causes problems.

Default

Disabled

Command Mode

Router configuration

Usage Guidelines

You can invoke authentication between two BGP peers, causing each segment sent on the TCP connection between them to be verified. This feature must be configured with the same password on both BGP peers; otherwise, the connection between them will not be made. The authentication feature uses the MD5 algorithm. Specifying this command causes the generation and checking of the MD5 digest on every segment sent on the TCP connection.

Configuring a password for a neighbor will cause an existing session to be torn down and a new one established.

If you specify a BGP peer group by using the *peer-group-name* argument, all of the members of the peer group will inherit the characteristic configured with this command.

If a router has a password configured for a neighbor, but the neighbor router does not, a message like the following will appear on the console while the routers attempt to establish a BGP session between them:

```
%TCP-6-BADAUTH: No MD5 digest from [peer's IP address]:11003 to [local router's
IP address]:179
```

Similarly, if the two routers have different passwords configured, a message like the following will appear on the console:

```
%TCP-6-BADAUTH: Invalid MD5 digest from [peer's IP address]:11004 to [local router's
IP address]:179
```

Example

The following example enables the authentication feature between this router and the BGP neighbor at 131.102.1.1. The password that must also be configured for the neighbor is *bla4u00=2nkq*.

```
router bgp 109
neighbor 131.108.1.1 password bla4u00=2nkq
```

Related Command

neighbor peer-group (creating)

neighbor peer-group (creating)

To create a BGP peer group, use the **neighbor peer-group** router configuration command. To remove the peer group and all of its members, use the **no** form of this command.

neighbor peer-group-name peer-group
no neighbor peer-group-name peer-group

Syntax Description

peer-group-name Name of the BGP peer group.

Default

There is no BGP peer group.

Command Mode

Router configuration

Usage Guidelines

Often in a BGP speaker, there are many neighbors configured with the same update policies (that is, same outbound route maps, distribute lists, filter lists, update source, and so on). Neighbors with the same update policies can be grouped into peer groups to simplify configuration and make update calculation more efficient.

Once a peer group is created with the **neighbor peer-group** command, it can be configured with the **neighbor** commands. By default, members of the peer group inherit all of the configuration options of the peer group. Members can also be configured to override the options that do not affect outbound updates.

Peer group members will always inherit the following: remote-as (if configured), version, update-source, out-route-map, out-filter-list, out-dist-list, minimum-advertisement-interval, and next-hop-self. All of the peer group members will inherit changes made to the peer group.

If a peer group is not configured with a remote-as, the members can be configured with the **neighbor {ip-address / peer-group-name} remote-as** command. This allows you to create peer groups containing EBGP neighbors.

Example for an IBGP Peer Group

In the following example, the peer group named *internal* configures the members of the peer group to be IBGP neighbors. By definition, this is an IBGP peer group because the **router bgp** command and the **neighbor remote-as** command indicate the same autonomous system (in this case, AS 100). All the peer group members use loopback 0 as the update source and use *set-med* as the outbound route-map. The inbound filter-list command shows that except 171.69.232.55 all the neighbor has filter-list 2 as the inbound filter list.

```
router bgp 100
neighbor internal peer-group
neighbor internal remote-as 100
neighbor internal update-source loopback 0
neighbor internal route-map set-med out
neighbor internal filter-list 1 out
neighbor internal filter-list 2 in
```

```
neighbor 171.69.232.53 peer-group internal
neighbor 171.69.232.54 peer-group internal
neighbor 171.69.232.55 peer-group internal
neighbor 171.69.232.55 filter-list 3 in
```

Example for an EBGP Peer Group

In the following example, the peer group *external-peers* is defined without the **neighbor remote-as** command. This is what makes it an EBGP peer group. Each individual member of the peer group is configured with its respective AS-number separately. Thus the peer group consists of members from autonomous systems 200, 300 and 400. All the peer group members have *set-metric* route map as an outbound route map and filter-list 99 as an outbound filter list. Except for neighbor 171.69.232.110, all of them have 101 as the inbound filter list.

```
router bgp 100
neighbor external-peers peer-group
neighbor external-peers route-map set-metric out
neighbor external-peers filter-list 99 out
neighbor external-peers filter-list 101 in
neighbor 171.69.232.90 remote-as 200
neighbor 171.69.232.90 peer-group external-peers
neighbor 171.69.232.100 remote-as 300
neighbor 171.69.232.100 peer-group external-peers
neighbor 171.69.232.110 remote-as 400
neighbor 171.69.232.110 peer-group external-peers
neighbor 171.69.232.110 filter-list 400 in
```

Related Commands

clear ip bgp peer-group
neighbor remote-as
neighbor peer-group (assigning members)
show ip bgp peer-group

neighbor peer-group (assigning members)

To configure a BGP neighbor to be a member of a peer group, use the **neighbor peer-group** router configuration command. To remove the neighbor from the peer group, use the **no** form of this command.

neighbor *ip-address* **peer-group** *peer-group-name*
no neighbor *ip-address* **peer-group** *peer-group-name*

Syntax Description

ip-address IP address of the BGP neighbor who belongs to the peer group specified by the *tag*.
peer-group-name Name of the BGP peer group to which this neighbor belongs.

Default

There are no BGP neighbors in a peer group.

Command Mode

Router configuration

Usage Guidelines

The neighbor at the IP address indicated inherits all the configured options of the peer group.

Example

In the following example,

```
router bgp 100
neighbor internal peer-group
neighbor internal remote-as 100
neighbor internal update-source loopback 0
neighbor internal route-map set-med out
neighbor internal filter-list 1 out
neighbor internal filter-list 2 in
neighbor 171.69.232.53 peer-group internal
neighbor 171.69.232.54 peer-group internal
neighbor 171.69.232.55 peer-group internal
neighbor 171.69.232.55 filter-list 3 in
```

Related Commands

neighbor peer-group (creating)
neighbor remote-as

neighbor remote-as

To add an entry to the BGP neighbor table, use the **neighbor remote-as** router configuration command. To remove an entry from the table, use the **no** form of this command.

```
neighbor {ip-address | peer-group-name} remote-as number
no neighbor {ip-address | peer-group-name} remote-as number
```

Syntax Description

<i>ip-address</i>	Neighbor's IP address.
<i>peer-group-name</i>	Name of a BGP peer group.
<i>number</i>	Autonomous system to which the neighbor belongs.

Default

There are no BGP neighbor peers.

Command Mode

Router configuration

Usage Guidelines

Specifying a neighbor with an autonomous system number that matches the autonomous system number specified in the **router bgp** global configuration command identifies the neighbor as internal to the local autonomous system. Otherwise, the neighbor is considered external.

If you specify a BGP peer group by using the *peer-group-name* argument, all of the members of the peer group will inherit the characteristic configured with this command.

Examples

The following example specifies that the router at the address 131.108.1.2 is a neighbor in autonomous system number 109:

```
router bgp 110
network 131.108.0.0
neighbor 131.108.1.2 remote-as 109
```

In the following example, a BGP router is assigned to autonomous system 109, and two networks are listed as originating in the autonomous system. Then the addresses of three remote routers (and their autonomous systems) are listed. The router being configured will share information about networks 131.108.0.0 and 192.31.7.0 with the neighbor routers. The first router listed is in the same Class B network address space, but in a different autonomous system; the second **neighbor** command illustrates specification of an internal neighbor (with the same autonomous system number) at address 131.108.234.2; and the last **neighbor** command specifies a neighbor on a different network.

```
router bgp 109
network 131.108.0.0
network 192.31.7.0
neighbor 131.108.200.1 remote-as 167
```

```
neighbor 131.108.234.2 remote-as 109
neighbor 150.136.64.19 remote-as 99
```

Related Command

neighbor peer-group (creating)

neighbor route-map

To apply a route map to incoming or outgoing routes, use the **neighbor route-map** router configuration command. To remove a route map, use the **no** form of this command.

```
neighbor {ip-address | peer-group-name} route-map route-map-name {in | out}  
no neighbor {ip-address | peer-group-name} route-map route-map-name {in | out}
```

Syntax Description

<i>ip-address</i>	Neighbor's IP address.
<i>peer-group-name</i>	Name of a BGP peer group.
<i>route-map-name</i>	Name of route map.
in	Apply to incoming routes.
out	Apply to outgoing routes.

Default

No route maps are applied to a peer.

Command Mode

Router configuration

Usage Guidelines

If an outbound route map is specified, it is proper behavior to only advertise routes that match at least one section of the route map.

If you specify a BGP peer group by using the *peer-group-name* argument, all of the members of the peer group will inherit the characteristic configured with this command. Specifying the command with an IP address will override the value inherited from the peer group.

Example

In the following example, route map “internal-map” is applied to incoming route from 198.92.70.24:

```
router bgp 5  
neighbor 198.92.70.24 route-map internal-map in  
!  
route-map internal-map  
match as-path 1  
set local-preference 100
```

Related Command

neighbor peer-group (creating)

neighbor send-community

To specify that a COMMUNITIES attribute should be sent to a BGP neighbor, use the **neighbor send-community** router configuration command. To remove the entry, use the **no** form of this command.

```
neighbor {ip-address | peer-group-name} send-community
no neighbor {ip-address | peer-group-name} send-community
```

Syntax Description

<i>ip-address</i>	Neighbor's IP address.
<i>peer-group-name</i>	Name of a BGP peer group.

Default

No COMMUNITIES attribute is sent to any neighbor.

Command Mode

Router configuration

Usage Guidelines

If you specify a BGP peer group by using the *peer-group-name* argument, all of the members of the peer group will inherit the characteristic configured with this command.

Example

In the following example, the router belongs to autonomous system 109 and is configured to send the COMMUNITIES attribute to its neighbor at IP address 198.92.70.23:

```
router bgp 109
neighbor 198.92.70.23 send-community
```

Related Commands

ip community-list
match community-list
neighbor peer-group (creating)
set community

neighbor third-party

To send updates regarding EGP third-party routers, use the **neighbor third-party** router configuration command. To disable these updates, use the **no** form of this command.

```
neighbor ip-address third-party third-party-ip-address [internal | external]  
no neighbor ip-address third-party third-party-ip-address [internal | external]
```

Syntax Description

<i>ip-address</i>	IP address of the EGP peer.
<i>third-party-ip-address</i>	Address of the third-party router on the network shared by the Cisco router and the EGP peer specified by <i>address</i> .
internal	(Optional) Indicates that the third-party router should be listed in the internal section of the EGP update. This is the default.
external	(Optional) Indicates that the third-party router should be listed in the external section of the EGP update.

Default

Disabled

Command Mode

Router configuration

Usage Guidelines

Using this *third-party mechanism*, EGP tells its peer that another router (the third party) on the shared network is the appropriate router for some set of destinations. If updates mentioning third-party routers are desired, use this command.

All networks reachable through the third-party router will be listed in the EGP updates as reachable by the router. The optional **internal** and **external** keywords indicate whether the third-party router should be listed in the internal or external section of the EGP update. Normally, all networks are mentioned in the internal section.

This command can be used multiple times to specify additional third-party routers.

Examples

In the following example, routes learned from router 131.108.6.99 will be advertised to 131.108.6.5 as third-party internal routes:

```
neighbor 131.108.6.5 third-party 131.108.6.99 internal
```

In the following example, routes learned from 131.108.6.100 will be advertised to 131.108.6.5 as third-party external routes:

```
neighbor 131.108.6.5 third-party 131.108.6.100 external
```

neighbor update-source

To have the router allow internal BGP sessions to use any operational interface for TCP connections, use the **neighbor update-source** router configuration command. To restore the interface assignment to the closest interface, which is called the best local address, use the **no** form of this command

neighbor { ip-address | peer-group-name } update-source interface
no neighbor { ip-address | peer-group-name } update-source interface

Syntax Description

<i>ip-address</i>	IP address of the BGP-speaking neighbor.
<i>peer-group-name</i>	Name of a BGP peer group.
<i>interface</i>	Loopback interface.

Default

Best local address

Command Mode

Router configuration

Usage Guidelines

This feature works in conjunction with the loopback interface feature described in the “Configuring Interfaces” chapter of the *Router Products Configuration Guide*.

If you specify a BGP peer group by using the *peer-group-name* argument, all of the members of the peer group will inherit the characteristic configured with this command.

Example

In the following example, BGP TCP connections for the specified neighbor will be sourced with loopback interface’s IP address rather than the best-local-address:

```
router bgp 110
network 160.89.0.0
neighbor 160.89.2.3 remote-as 110
neighbor 160.89.2.3 update-source Loopback0
```

Related Command

neighbor peer-group (creating)

neighbor version

To configure the router to accept only a particular BGP version, use the **neighbor version** router configuration command. To use the default version level of a neighbor, use the **no** form of this command.

```
neighbor {ip-address | peer-group-name} version value  
no neighbor {ip-address | peer-group-name} version value
```

Syntax Description

<i>ip-address</i>	IP address of the BGP-speaking neighbor.
<i>peer-group-name</i>	Name of a BGP peer group.
<i>value</i>	BGP version number. The version can be set to 2 to force the router to only use Version 2 with the specified neighbor. The default is to use Version 4 and dynamically negotiate down to Version 2 if requested.

Default

BGP Version 4

Command Mode

Router configuration

Usage Guidelines

Entering this command disables dynamic version negotiation.

Our implementation of BGP supports BGP Versions 2, 3, and 4. If the neighbor does not accept default Version 4, dynamic version negotiation is implemented to negotiate down to Version 2.

If you specify a BGP peer group by using the *peer-group-name* argument, all of the members of the peer group will inherit the characteristic configured with this command.

Example

The following example locks down to Version 4 of the BGP protocol:

```
router bgp 109
neighbor 131.104.27.2 version 4
```

Related Command

neighbor peer-group (creating)

neighbor weight

To assign a weight to a neighbor connection, use the **neighbor weight** router configuration command. To remove a weight assignment, use the **no** form of this command.

```
neighbor {ip-address | peer-group-name} weight weight
no neighbor {ip-address | peer-group-name} weight weight
```

Syntax Description

<i>ip-address</i>	Neighbor's IP address.
<i>peer-group-name</i>	Name of a BGP peer group.
<i>weight</i>	Weight to assign. Acceptable values are 0 to 65535.

Default

Routes learned through another BGP peer have a default weight of 0 and routes sourced by the local router have a default weight of 32768.

Command Mode

Router configuration

Usage Guidelines

All routes learned from this neighbor will have the assigned weight initially. The route with the highest weight will be chosen as the preferred route when multiple routes are available to a particular network.

The weights assigned with the **match as-path** and **set weight** route-map commands override the weights assigned using the **neighbor weight** and **neighbor filter-list** commands.

Note For weight changes to take effect, it may be necessary to use **clear ip bgp ***.

If you specify a BGP peer group by using the *peer-group-name* argument, all of the members of the peer group will inherit the characteristic configured with this command.

Example

The following example sets the weight of all routes learned via 151.23.12.1 to 50:

```
router bgp 109
neighbor 151.23.12.1 weight 50
```

Related Commands

neighbor distribute-list

neighbor filter-list

neighbor peer-group (creating)

net

To configure a Network Entity Title (NET) for the routing process, use the **net** router configuration command. To remove a NET, use the **no** form of this command.

```
net network-entity-title  
no net network-entity-title
```

Syntax Description

<i>network-entity-title</i>	NET that specifies the area address and the system ID for an IS-IS routing process. This argument can be either an address or a name.
-----------------------------	---

Default

No NET is configured.

Command Mode

Router configuration

Usage Guidelines

For IS-IS, multiple NETs per router are allowed, with a maximum of three. There is no default value for this command.

Example

The following example specifies a single NET:

```
router isis Pieinthesky  
net 47.0004.004d.0001.0000.0c11.1111.00
```

network (BGP)

To specify the list of networks for the BGP routing process, use this form of the **network** router configuration command. To remove an entry, use the **no** form of this command.

```
network network-number [mask network-mask]
no network network-number [mask network-mask]
```

Syntax Description

<i>network-number</i>	IP address of a peer router with which routing information will be exchanged.
<i>network-mask</i>	(Optional) Network mask address.

Default

No networks are specified.

Command Mode

Router configuration

Usage Guidelines

These types of networks can be learned from connected routes, dynamic routing, and from static route sources.

A maximum of 200 **network** commands may be specified for a single BGP process.

Example

The following example sets up network 131.108.0.0 to be included in the router's BGP updates:

```
router bgp 120
network 131.108.0.0
```

Related Commands

network backdoor
network mask
network weight
router bgp

network (EGP)

To specify the list of networks for the EGP routing process, use this form of the **network** router configuration command. To remove an entry, use the **no** form of this command.

```
network network-number  
no network network-number
```

Syntax Description

<i>network-number</i>	IP address of a peer router with which routing information will be exchanged.
-----------------------	---

Default

No networks are specified.

Command Mode

Router configuration

Usage Guidelines

The networks to be advertised to the EGP peers of an EGP routing process are advertised with a distance of zero. The restrictions on the network you specify are that it must appear in the routing table, and the network number must not contain any subnet information. The network can be connected, statically configured, or redistributed into EGP from other routing protocols. Multiple commands can be used to specify additional networks.

Example

The following example illustrates a typical configuration for an EGP router process. The router is in autonomous system 109 and is peering with routers in autonomous system 164. It will advertise the networks 131.108.0.0 and 192.31.7.0 to the router in autonomous system 164, 10.2.0.2. The information sent and received from peer routers can be filtered in various ways, including blocking information from certain routers and suppressing the advertisement of specific routes.

```
autonomous-system 109  
router egp 164  
network 131.108.0.0  
network 192.31.7.0  
neighbor 10.2.0.2
```

Related Command

router egp

network (IGRP and Enhanced IGRP)

To specify a list of networks for the Enhanced IGRP routing process, use this form of the **network** router configuration command. To remove an entry, use the **no** form of this command.

```
network network-number  
no network network-number
```

Syntax Description

<i>network-number</i>	IP address of the directly connected networks.
-----------------------	--

Default

No networks are specified.

Command Mode

Router configuration

Usage Guidelines

The network number specified must not contain any subnet information. You can specify multiple **network** commands.

IGRP or Enhanced IGRP sends updates to the interfaces in the specified network(s). Also, if an interface's network is not specified, it will not be advertised in any IGRP or Enhanced IGRP update.

Example

The following example configures a router for IGRP and assigns autonomous system 109. The **network** commands indicate the networks directly connected to the router.

```
router igrp 109  
network 131.108.0.0  
network 192.31.7.0
```

Related Commands

router igrp
router eigrp

network (RIP)

To specify a list of networks for the RIP routing process, use this form of the **network** router configuration command. To remove an entry, use the **no** form of this command.

network *network-number*
no network *network-number*

Syntax Description

network-number IP address of the network of directly connected networks.

Default

No networks are specified.

Command Mode

Router configuration

Usage Guidelines

The network number specified must not contain any subnet information. You can specify multiple **network** commands. RIP routing updates will be sent and received only through interfaces on this network.

RIP sends updates to the interfaces in the specified network(s). Also, if an interface's network is not specified, it will not be advertised in any RIP update.

Example

The following example defines RIP as the routing protocol to be used on all interfaces connected to networks 128.99.0.0 and 192.31.7.0:

```
router rip
network 128.99.0.0
network 192.31.7.0
```

Related Command

router rip

network area

To define the interfaces on which OSPF runs and to define the area ID for those interfaces, use the **network area** router configuration command. To disable OSPF routing for interfaces defined with the *address wildcard-mask* pair, use the **no** form of this command.

network address wildcard-mask area area-id
no network address wildcard-mask area area-id

Syntax Description

<i>address</i>	IP address.
<i>wildcard-mask</i>	IP-address-type mask that includes “don’t care” bits.
<i>area-id</i>	Area that is to be associated with the OSPF address range. It can be specified as either a decimal value or as an IP address. If you intend to associate areas with IP subnets, you can specify a subnet address as the <i>area-id</i> .

Default

Disabled

Command Mode

Router configuration

Usage Guidelines

The *address* and *wildcard-mask* arguments together allow you to define one or multiple interfaces to be associated with a specific OSPF area using a single command. Using the *wildcard-mask* allows you to define one or multiple interfaces to be associated with a specific OSPF area using a single command. If you intend to associate areas with IP subnets, you can specify a subnet address as the *area-id*.

The router sequentially evaluates the *address/wildcard-mask* pair for each interface as follows:

- 1 The *wildcard-mask* is logically ORed with the interface IP address.
- 2 The *wildcard-mask* is logically ORed with *address* in the **network** command.
- 3 The router compares the two resulting values.
- 4 If they match, OSPF is enabled on the associated interface and this interface is attached to the OSPF area specified.

Note Any individual interface can only be attached to a single area. If the address ranges specified for different areas overlap, the router will adopt the first area in the **network** command list and ignore the subsequent overlapping portions. In general, it is recommended that you devise address ranges that do not overlap in order to avoid inadvertent conflicts.

Example

In the following partial example, OSPF routing process 109 is initialized, and four OSPF areas are defined: 10.9.50.0, 2, 3, and 0. Areas 10.9.50.0, 2, and 3 mask specific address ranges, while area 0 enables OSPF for all other networks.

```
router ospf 109
network 131.108.20.0 0.0.0.255 area 10.9.50.0
network 131.108.0.0 0.0.255.255 area 2
network 131.109.10.0 0.0.0.255 area 3
network 0.0.0.0 255.255.255.255 area 0
```

Related Command

router ospf

network backdoor

To specify a backdoor route to a BGP border router that will provide better information about the network, use the **network backdoor** router configuration command. To remove an address from the list, use the **no** form of this command.

network address backdoor
no network address backdoor

Syntax Description

address IP address of the network to which you want a backdoor route.

Default

No network is advertised.

Command Mode

Router configuration

Usage Guidelines

A backdoor network is treated as a local network, except that it is not advertised.

Example

The following example configures network 131.108.0.0 as a local network and network 192.31.7.0 as a backdoor network:

```
router bgp 109
network 131.108.0.0
network 192.31.7.0 backdoor
```

network weight

To assign an absolute weight to a BGP network, use the **network weight** router configuration command. To delete an entry, use the **no** form of the command.

```
network address weight weight  
no network address weight weight
```

Syntax Description

<i>address</i>	IP address of the network.
<i>weight</i>	Absolute weight, or importance. It can be an integer from 0 to 65535.

Default

Weight is unmodified. Weight is zero if the original default weight has not been modified by other router configuration commands.

Command Mode

Router configuration

Usage Guidelines

The weight specified by this command overrides a weight assigned by the **redistribute** command.

Example

In the following example, the BGP network has a weight of 100:

```
router bgp 5  
network 193.0.0.0 weight 100
```

offset-list

To add an offset to incoming and outgoing metrics to routes learned via RIP and IGRP, use the **offset-list** router configuration command. To remove an offset list, use the **no** form of this command.

```
offset-list {in | out} offset [access-list-number | [type number]]
no offset-list {in | out} offset [access-list-number | [type number]]
```

Syntax Description

in	Applies the access list to incoming metrics.
out	Applies the access list to outgoing metrics.
<i>offset</i>	Positive offset to be applied to metrics for networks matching the access list. If the offset is 0, no action is taken.
<i>access-list-number</i>	(Optional) Access list to be applied. If unspecified, the argument supplied to <i>offset</i> is applied to all metrics. If <i>offset</i> is 0, no action is taken. For IGRP, the offset is added to the delay component only. Must be a standard access list.
<i>type</i>	(Optional) Interface type to which the offset-list is applied.
<i>number</i>	(Optional) Interface number to which the offset-list is applied.

Default

Disabled

Command Mode

Router configuration

Usage Guidelines

The offset value is added to the routing metric. An offset-list with an interface type and interface number is considered extended and takes precedence over an offset-list that is not extended. Therefore, if an entry passes the extended offset-list and the normal offset-list, the extended offset-list's offset is added to the metric.

Examples

The following example applies an offset of 10 to the router's delay component for all outgoing metrics:

```
offset-list out 10
```

In the following example, the router applies the same offset in the previous example only to access list 121:

```
offset-list out 10 121
```

In the following example of an extended offset-list, the router applies the offset of 10 to routes learned from Ethernet interface 0:

```
offset-list in 10 ethernet 0
```

ospf auto-cost-determination

To control how OSPF calculates default metrics for the interface, use the **ospf auto-cost-determination** router configuration command. To disable this feature, use the **no** form of this command.

ospf auto-cost-determination
no ospf auto-cost-determination

Syntax Description

This command has no arguments or keywords.

Default

Enabled

Command Mode

Router configuration

Usage Guidelines

In Cisco IOS Release 10.2 and earlier, OSPF assigns default OSPF metrics to interfaces regardless of the interface bandwidth. It gives both 64K and T1 links the same metric (1562), and thus requires an explicit **ip ospf cost** command in order to take advantage of the faster link.

In Cisco IOS Release 10.3 and later, by default OSPF will calculate the OSPF metric for an interface according to the bandwidth of the interface. For example, a 64K link will get a metric of 1562, while a T1 link will have a metric of 64.

The OSPF metric is calculated as *metric-scale / bandwidth*, with *metric-scale* equal to 10^8 by default, giving FDDI a metric of 1.

Example

The following example causes a fixed default metric assignment, regardless of interface bandwidth:

```
router ospf 1
no ospf auto-cost-determination
```

Related Command

ip ospf cost

passive-interface

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

```
passive-interface type number
no passive-interface type number
```

Syntax Description

<i>type</i>	Interface type.
<i>number</i>	Interface number.

Default

Routing updates are sent on the interface.

Command Mode

Router configuration

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.

For OSPF, 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 IS-IS, 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.

Enhanced IGRP 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 131.108.0.0 except Ethernet interface 1:

```
router igrp 109
network 131.108.0.0
passive-interface ethernet 1
```

The following configuration enables IS-IS on interfaces Ethernet 1 and serial 0 and advertises the IP addresses of Ethernet 0 in its Link State PDUs:

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

redistribute

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

```
redistribute protocol [process-id] {level-1 | level-1-2 | level-2} [metric metric-value]
[metric-type type-value] [match {internal | external 1 | external 2}]
[tag tag-value] [route-map map-tag] [weight weight] [subnets]
no redistribute protocol [process-id] {level-1 | level-1-2 | level-2} [metric metric-value]
[metric-type type-value] [match {internal | external 1 | external 2}]
[tag tag-value] [route-map map-tag] [weight weight] [subnets]
```

Syntax Description

<i>protocol</i>	Source protocol from which routes are being redistributed. It can be one of the following keywords: bgp , egp , igrp , isis , ospf , static [ip] , connected , and rip .
	The keyword static [ip] is used to redistribute IP static routes. The optional ip keyword is used when redistributing into IS-IS.
	The keyword connected refers to routes which are established automatically by virtue of having enabled IP on an interface. For routing protocols such as OSPF and IS-IS, these routes will be redistributed as external to the autonomous system.
<i>process-id</i>	(Optional) For bgp , egp , or igrp , this is an autonomous system number, which is a 16-bit decimal number. For isis , this is an optional <i>tag</i> 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 ospf , 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 rip , no <i>process-id</i> value is needed.
level-1	For IS-IS, Level 1 routes are redistributed into other IP routing protocols independently.
level-1-2	For IS-IS, both Level 1 and Level 2 routes are redistributed into other IP routing protocols.
level-2	For IS-IS, Level 2 routes are redistributed into other IP routing protocols independently.
metric <i>metric-value</i>	(Optional) Metric used for the redistributed route. If a value is not specified for this option, and no value is specified using the default-metric command, the default metric value is 0. Use a value consistent with the destination protocol.

metric-type <i>type-value</i>	(Optional) For OSPF, 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 router adopts a Type 2 external route. For IS-IS, it can be one of two values: internal —IS-IS metric which is < 63. external —IS-IS metric which is > 64 < 128. The default is internal .
match {internal external 1 external 2}	(Optional) For OSPF, 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.
tag <i>tag-value</i>	(Optional) 32-bit decimal value attached to each external route. This is not used by the OSPF protocol itself. It may be used to communicate information between Autonomous System Boundary Routers. If none is specified, then the remote autonomous system number is used for routes from BGP and EGP; for other protocols, zero (0) is used.
route-map	(Optional) Route map 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.
weight <i>weight</i>	(Optional) Network weight when redistributing into BGP. An integer between 0 and 65535.
subnets	(Optional) For redistributing routes into OSPF, the scope of redistribution for the specified protocol.

Default

Route redistribution is disabled.

Command Mode

Router configuration

Usage Guidelines

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

A router receiving a link-state protocol (LSP) 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 keyword **level-1-2** allows both in a single command.

Redistributed routing information should always be filtered by the **distribute-list out** router configuration command. This 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 Autonomous System Boundary Router (ASBR). However, an ASBR does not, by default, generate a *default route* into the OSPF routing domain.

When routes are redistributed between OSPF processes, no OSPF metrics are preserved.

When routes are redistributed into OSPF and no metric is specified in the **metric** keyword, the default metric that OSPF uses is 20 for routes from all protocols except BGP route, which gets a metric of 1.

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

The only **connected** routes affected by this **redistribute** command are the routes not specified by the **network** 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 **default-information originate** is specified.

Examples

The following are examples of the various configurations you would use to redistribute one routing protocol into another routing protocol.

The following example configuration causes OSPF routes to be redistributed into a BGP domain:

```
router bgp 109
  redistribute ospf...
```

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

```
router ospf 110
  redistribute igrp...
```

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

```
router ospf 109
 redistribute igrp 108 metric 100 subnets
 redistribute rip metric 200 subnets
```

In the following example, BGP routes are configured 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 isis
 redistribute bgp 120 metric 5 metric-type external
```

Related Commands

default-information originate (BGP)
default-information originate (EGP)
default-information originate (IS-IS)
default-information originate (OSPF)
distribute-list out
route-map
show route-map

route-map

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

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

Syntax Description

map-tag Defines 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 **permit** 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 **permit** 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 **deny** is specified, the route is not redistributed or 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, it reverts to the normal forwarding algorithm.

sequence-number (Optional) Number that indicates the position a new route map is to have in the list of route maps already configured with the same name. If given with the **no** form of this command, it specifies the position of the route map that should be deleted.

Default

No default is available.

Command Mode

Global configuration

Usage Guidelines

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**. 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 related **match** commands are listed in the section “Related Commands for Redistribution.” 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 following example as 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** command, in addition to the **route-map** command, and the **match** and **set** commands to define the conditions for policy routing packets. The related **match** and **set** commands are listed in the section “Related Commands for Policy Routing.” 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.

Examples

The following example redistributes all OSPF routes into IGRP:

```
router igrp 109
redistribute ospf 110
  default metric 1000 100 255 1 1500
```

The following example redistributes RIP routes with a hop count equal to 1 into OSPF. These routes will be redistributed into OSPF as external link state advertisements with a metric of 5, metric type of Type 1 and a tag equal to 1.

```
router ospf 109
redistribute rip route-map rip-to-ospf

route-map rip-to-ospf permit
  match metric 1
  set metric 5
  set metric-type type1
  set tag 1
```

Related Commands for Redistribution

match as-path
match community-list
match interface
match ip address

```
match ip next-hop
match ip route-source
match metric
match route-type
match tag
set as-path
set automatic-tag
set community
set level
set local-preference
set metric
set metric-type
set next-hop
set origin
set tag
set weight
show route-map
```

Related Commands for Policy Routing

```
ip policy route-map
match ip address
match length
set default interface
set interface
set ip default next-hop
set ip next-hop
```

router bgp

To configure the Border Gateway Protocol (BGP) routing process, use the **router bgp** global configuration command. To remove a routing process, use the **no** form of this command.

```
router bgp autonomous-system
no router bgp autonomous-system
```

Syntax Description

<i>autonomous-system</i>	Number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along.
--------------------------	---

Default

No BGP routing process is enabled by default.

Command Mode

Global configuration

Usage Guidelines

This command allows you to set up a distributed routing core that automatically guarantees the loop-free exchange of routing information between autonomous systems.

Example

The following example configures a BGP process for autonomous system 120:

```
router bgp 120
```

Related Commands

neighbor
network (BGP)
timers bgp

router egp

To configure the Exterior Gateway Protocol (EGP) routing process, use the **router egp** global configuration command. To turn off an EGP routing process, use the **no router egp** command.

```
router egp remote-as  
no router egp remote-as
```

Syntax Description

<i>remote-as</i>	Autonomous system number the router expects its peers to be advertising in their EGP messages.
------------------	--

Default

No EGP routing process is defined.

Command Mode

Global configuration

Usage Guidelines

You must specify the autonomous system number before starting EGP. The local autonomous system number will be included in EGP messages sent by the router. The software does not insist that the actual remote autonomous system number match the configured autonomous system numbers. The output from the **debug ip-egp** EXEC command will advise of any discrepancies.

Example

The following example assigns a router to autonomous system 109 and is peering with routers in autonomous system 164:

```
autonomous-system 109  
router egp 164
```

Related Commands

autonomous-system (EGP)
neighbor
network (EGP)
timers egp

router egp 0

To specify that a router should be considered a core gateway, use the **router egp 0** global configuration command. To disable this function, use the **no** form of this command.

```
router egp 0
no router egp 0
```

Syntax Description

This command has no arguments or keywords.

Default

Disabled

Command Mode

Global configuration

Usage Guidelines

Core gateways are central clearinghouses of routing information. Only one core gateway process can be configured in a router.

The **router egp 0** global configuration command allows a specific router to have an EGP process that will enable it to act as a peer with any reachable autonomous system and information is exchanged freely between autonomous systems.

Normally, an EGP process expects to communicate with neighbors from a single autonomous system. Because all neighbors are in the same autonomous system, the EGP process assumes that these neighbors all have consistent internal information. Therefore, if the EGP process is informed about a route from one of its neighbors, it will not send it out to other neighbors.

With *core EGP*, the assumption is that all neighbors are from different autonomous systems, and all have inconsistent information. In this case, the EGP process distributes routes from one neighbor to all others (but not back to the originator). This allows the EGP process to be a central clearinghouse for information.

To control how an EGP process determines which neighbors will be treated as peers, use the **neighbor any** router configuration command with the **router egp 0** global configuration command.

Example

The following example illustrates how an EGP core gateway can be configured:

```
access-list 1 permit 10.0.0.0 0.255.255.255
! global access list assignment
router egp 0
neighbor any 1
network 131.108.0.0
```

Related Commands

neighbor any
neighbor any third-party

router eigrp

To configure the Enhanced IGRP routing process, use the **router eigrp** global configuration command. To shut down a routing process, use the **no** form of this command.

```
router eigrp process-id
no router eigrp process-id
```

Syntax Description

<i>process-id</i>	Number of a process that identifies the routes to the other Enhanced IGRP routers. It is also used to tag the routing information. If you have an autonomous system number, you can use it for the process number.
-------------------	--

Default

Disabled

Command Mode

Global configuration

Example

The following example shows how to configure an Enhanced IGRP routing process and assign process number 109:

```
router eigrp 109
```

Related Command

network (IGRP and Enhanced IGRP)

router igrp

To configure the Interior Gateway Routing Protocol (IGRP) routing process, use the **router igrp** global configuration command. To shut down an IGRP routing process, use the **no** form of this command.

```
router igrp process-id  
no router igrp process-id
```

Syntax Description

<i>process-id</i>	Number of a process that identifies the routes to the other IGRP routers. It is also used to tag the routing information. If you have an autonomous system number, you can use it for the process number.
-------------------	---

Default

No IGRP routing process is defined.

Command Mode

Global configuration

Usage Guidelines

It is not necessary to have a registered autonomous system number to use IGRP. If you do not have a registered number, you are free to create your own. We recommend that if you do have a registered number, you use it to identify the IGRP process.

Example

The following example shows how to configure an IGRP routing process and assign process number 109:

```
router igrp 109
```

Related Command

network (IGRP and Enhanced IGRP)

router isis

To enable the IS-IS routing protocol and to specify an IS-IS process for IP, use the **router isis** global configuration command. To disable IS-IS routing, use the **no** form of this command.

```
router isis [tag]  
no router isis [tag]
```

Syntax Description

<i>tag</i>	(Optional) Meaningful name for a routing process. If it is not specified, a null tag is assumed and the process is referenced with a null tag. This name must be unique among all IP router processes for a given router.
------------	---

Default

Disabled

Command Mode

Global configuration

Usage Guidelines

You can specify only one IS-IS process per router. Only one IS-IS process is allowed whether you run it in integrated mode, ISO CLNS only, or IP only.

Example

The following example configures the router for IP routing and enables the IS-IS routing protocol:

```
ip routing  
router isis
```

Related Commands

ip router isis
net

router ospf

To configure an OSPF routing process, use the **router ospf** global configuration command. To terminate an OSPF routing process, use the **no** form of this command.

```
router ospf process-id  
no router ospf process-id
```

Syntax Description

<i>process-id</i>	Internally used identification parameter for an OSPF routing process. It is locally assigned and can be any positive integer. A unique value is assigned for each OSPF routing process.
-------------------	---

Default

No OSPF routing process is defined.

Command Mode

Global configuration

Usage Guidelines

You can specify multiple OSPF routing processes in each router.

Example

The following example shows how to configure an OSPF routing process and assign a process number of 109:

```
router ospf 109
```

Related Command

network area

router rip

To configure the Routing Information Protocol (RIP) routing process, use the **router rip** global configuration command. To turn off the RIP routing process, use the **no** form of this command.

```
router rip
no router rip
```

Syntax Description

This command has no arguments or keywords.

Default

No RIP routing process is defined.

Command Mode

Global configuration

Example

The following example shows how to begin the RIP routing process:

```
router rip
```

Related Command

network (RIP)

set as-path

To modify an autonomous system path for BGP routes, use the **set as-path** route map configuration command. To not modify the autonomous system path, use the **no** form of this command.

```
set as-path {tag | prepend as-path-string}  
no set as-path {tag | prepend as-path-string}
```

Syntax Description

tag Converts the tag of a route into an autonomous system path. Applies only when redistributing routes into BGP.

prepend *as-path-string* Appends the string following the keyword **prepend** to the as-path of the route that is matched by the route map. Applies to inbound and outbound BGP route maps.

Default

Autonomous system path is not modified.

Command Mode

Route map configuration

Usage Guidelines

The only global BGP metric available to influence the best path selection is the AS-PATH length. By varying the length of the AS-PATH, a BGP speaker can influence the best path selection by a peer further away.

By allowing you to convert the tag into an autonomous system path, the **set as-path tag** variation of this command modifies the autonomous system length. The **set as-path prepend** variation allows you to prepend an arbitrary autonomous system path string to BGP routes. Usually the local autonomous system number is prepended multiple times. This increases the autonomous system path length.

Examples

The following example converts the tag of a redistributed route into an autonomous system path:

```
route-map set-as-path-from-tag  
match as-path 2  
set as-path prepend 100 100 100  
!  
router bgp 100  
redistribute ospf 109 route-map set-as-path-from-tag
```

The following example prepends 100 100 100 to all the routes advertised to 131.108.1.1:

```
route-map set-as-path  
match as-path 1  
set as-path prepend 100 100 100  
!  
router bgp 100  
neighbor 131.108.1.1 route-map set-as-path out
```

Related Commands

match as-path
match community-list
match interface
match ip address
match ip next-hop
match ip route-source
match metric
match route-type
match tag
route-map
set automatic-tag
set community
set level
set local-preference
set metric
set metric-type
set next-hop
set origin
set tag
set weight

set automatic-tag

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

set automatic-tag
no set automatic-tag

Syntax Description

This command has no arguments or keywords.

Default

Disabled

Command Mode

Route-map configuration

Usage Guidelines

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

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

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

Example

In the following example, the router is configured to automatically compute the tag value for the BGP learned routes:

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

Related Commands

match as-path
match community-list
match interface
match ip address
match ip next-hop
match ip route-source

match metric
match route-type
match tag
route-map
set as-path
set community
set level
set local-preference
set metric
set metric-type
set next-hop
set origin
set tag
set weight

set community

To set the BGP COMMUNITIES attribute, use the **set community** route-map configuration command. To delete the entry, use the **no** form of this command.

```
set community community-number [additive]  
no set community community-number [additive]
```

Syntax Description

community-number Valid values are 1 through 4294967200, **no-export**, or **no-advertise**.

additive (Optional) Adds the community to the already existing communities.

Default

No BGP COMMUNITIES attributes exist.

Command Mode

Route-map configuration

Usage Guidelines

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

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

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

Example

In the following example, routes that pass the autonomous system path access list 1 have the community set to 109. Routes that pass the autonomous system path access list 2 have the community set to no-export (these routes will not be advertised to any EBGP peers).

```
route-map set_community 10 permit  
match as-path 1  
set community 109  
  
route-map set_community 20 permit  
match as-path 2  
set community no-export
```

Related Commands

ip community-list
match community-list
route-map

set default interface

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

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

Syntax Description

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

Default

Disabled

Command Mode

Route-map configuration

Usage Guidelines

Use this command to provide certain users a different default route. If the router has no explicit route for the destination, then it routes the packet to this interface. The first interface specified with the **set default interface** command that is up is used. The optionally specified interfaces are tried in turn.

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

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

```
set ip next-hop
set interface
set ip default next-hop
set default interface
```

Example

In the following example, packets that have a Level 3 length of 3 to 50 bytes and for which the router has no explicit route to the destination are output to Ethernet interface 0:

```
interface serial 0
ip policy route-map brighton
!
route-map brighton
match length 3 50
set default interface ethernet 0
```

Related Commands

ip policy route-map
match ip address
match length
route-map
set interface
set ip default next-hop
set ip next-hop

set interface

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

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

Syntax Description

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

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

Default

Disabled

Command Mode

Route-map configuration

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.

If the first interface specified with the **set interface** command is down, the optionally specified interfaces are tried in turn.

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

```
set ip next-hop  
set interface  
set ip default next-hop  
set default interface
```

A useful next hop implies an interface. As soon as a next hop and an interface are found, the packet is routed.

Specifying **set interface null 0** is a way to write a policy that the packet be dropped and an “unreachable” message be generated.

Example

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

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

Related Commands

ip policy route-map
match ip address
match length
route-map
set default interface
set ip default next-hop
set ip next-hop

set ip default next-hop

To indicate where to output packets that pass a match clause of a route map for policy routing and for which the router has no explicit route to a destination, use the **set ip default next-hop** route-map configuration command. To delete an entry, use the **no** form of this command.

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

Syntax Description

ip-address IP address of the next hop to which packets are output. It need not be an adjacent router.

Default

Disabled

Command Mode

Route-map configuration

Usage Guidelines

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

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

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

```
set ip next-hop  
set interface  
set ip default next-hop  
set default interface
```

Example

The following example provides two sources with equal access to two different service providers. Packets arriving on async interface 1 from the source 1.1.1.1 are sent to the router at 6.6.6.6 if the router has no explicit route for the packet's destination. Packets arriving from the source 2.2.2.2 are sent to the router at 7.7.7.7 if the router has no explicit route for the packet's destination. All other packets for which the router has no explicit route to the destination are discarded.

```
access-list 1 permit ip 1.1.1.1 0.0.0.0  
access-list 2 permit ip 2.2.2.2 0.0.0.0
```

```
!
interface async 1
ip policy route-map equal-access
!
route-map equal-access permit 10
match ip address 1
set ip default next-hop 6.6.6.6
route-map equal-access permit 20
match ip address 2
set ip default next-hop 7.7.7.7
route-map equal-access permit 30
set default interface null0
```

Related Commands

ip policy route-map
match ip address
match length
route-map
set default interface
set interface
set ip next-hop

set ip next-hop

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

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

Syntax Description

<i>ip-address</i>	IP address of the next hop to which packets are output. It need not be an adjacent router.
-------------------	--

Default

Disabled

Command Mode

Route-map configuration

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.

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

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

```
set ip next-hop  
set interface  
set ip default next-hop  
set default interface
```

Example

In the following example, packets with a Level 3 length of 3 to 50 bytes are output to the router at IP address 161.14.2.2:

```
interface serial 0  
ip policy route-map thataway  
!  
route-map thataway  
match length 3 50  
set ip next-hop 161.14.2.2
```

Related Commands

ip policy route-map
match ip address
match length
route-map
set default interface
set interface
set ip default next-hop

set level

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

```
set level {level-1 | level-2 | level-1-2 | stub-area | backbone}
no set level {level-1 | level-2 | level-1-2 | stub-area | backbone}
```

Syntax Description

level-1	Imports routes into a Level-1 area.
level-2	Imports routes into Level-2 subdomain.
level-1-2	Imports routes into Level-1 and Level-2.
stub-area	Imports routes into OSPF NSSA area.
backbone	Imports routes into OSPF backbone area.

Default

Disabled

For IS-IS destinations, the default value is **level-2**. For OSPF destinations, the default value is **backbone**.

Command Mode

Route-map configuration

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**. The **set** commands specify the *set actions*—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

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

Example

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

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

Related Commands

match as-path
match community-list
match interface
match ip address
match ip next-hop
match ip route-source
match metric
match route-type
match tag
route-map
set as-path
set automatic-tag
set community
set local-preference
set metric
set metric-type
set next-hop
set origin
set tag
set weight

set local-preference

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

```
set local-preference value
no set local-preference value
```

Syntax Description

<i>value</i>	Preference value. An integer from 0 through 4294967295.
--------------	---

Default

Preference value of 100

Command Mode

Route-map configuration

Usage Guidelines

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

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

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

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

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

Example

In the following example, the local preference is set to 100 for all routes that are included in access list 1:

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

Related Commands

bgp default local-preference
match as-path
match community-list
match interface

match ip address
match ip next-hop
match ip route-source
match metric
match route-type
match tag
route-map
set as-path
set automatic-tag
set community
set level
set metric
set metric-type
set next-hop
set origin
set tag
set weight

set metric

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

set metric *metric-value*
no set metric *metric-value*

Syntax Description

metric-value Metric value or IGRP bandwidth in kilobits per second. It can be an integer from -294967295 through 294967295.

Default

Default metric value.

Command Mode

Route-map configuration

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**. The **set** commands specify the *set actions*—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

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

Example

In the following example, the metric value for the destination routing protocol is set to 100:

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

Related Commands

match as-path
match community-list
match interface
match ip address
match ip next-hop
match ip route-source
match metric
match route-type
match tag
route-map

set as-path
set automatic-tag
set community
set level
set local-preference
set metric-type
set next-hop
set origin
set tag
set weight

set metric-type

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

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

Syntax Description

internal	IS-IS internal metric.
external	IS-IS external metric.
type-1	OSPF external type 1 metric.
type-2	OSPF external type 2 metric.

Default

Disabled

Command Mode

Route-map configuration

Usage Guidelines

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

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

Example

In the following example, the metric type of the destination protocol is set to OSPF external type 1:

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

Related Commands

match as-path
match community-list
match interface
match ip address
match ip next-hop

```
match ip route-source
match metric
match route-type
match tag
route-map
set as-path
set automatic-tag
set community
set level
set local-preference
set metric
set next-hop
set origin
set tag
set weight
```

set next-hop

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

```
set next-hop next-hop  
no set next-hop next-hop
```

Syntax Description

<i>next-hop</i>	IP address of the next hop router.
-----------------	------------------------------------

Default

Default next-hop address.

Command Mode

Route-map configuration

Usage Guidelines

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

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

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

Example

In the following example, routes that pass the access list have the next hop set to 198.92.70.24:

```
route-map map_hop  
match address 5  
set next-hop 198.92.70.24
```

Related Commands

match as-path
match community-list
match interface
match ip address
match ip next-hop
match ip route-source
match metric
match route-type

match tag
route-map
set as-path
set automatic-tag
set community
set level
set local-preference
set metric
set metric-type
set origin
set tag
set weight

set origin

To set the BGP origin code, use the **set origin** route-map configuration command. To delete an entry, use the **no** form of this command.

```
set origin {igp | egp autonomous-system | incomplete}
```

Syntax Description

igp	Remote IGP.
egp	Local EGP.
<i>autonomous-system</i>	Remote autonomous system. This is an integer from 0 through 65535.
incomplete	Unknown heritage.

Default

Default origin, based on route in main IP routing table.

Command Mode

Route-map configuration

Usage Guidelines

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

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

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

Example

In the following example, routes that pass the route map have the origin set to IGP:

```
route-map set_origin
  match as-path 10
  set origin igp
```

Related Commands

match as-path
match community-list
match interface
match ip address

```
match ip next-hop
match ip route-source
match metric
match route-type
match tag
route-map
set as-path
set automatic-tag
set community
set level
set local-preference
set metric
set metric-type
set next-hop
set tag
set weight
```

set tag

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

```
set tag tag-value
no set tag tag-value
```

Syntax Description

<i>tag-value</i>	Name for the tag. Integer from 0 through 4294967295.
------------------	--

Default

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

Command Mode

Route-map configuration

Usage Guidelines

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

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

Example

In the following example, the tag value of the destination routing protocol is set to 5:

```
route-map tag
  set tag 5
```

Related Commands

match as-path
match community-list
match interface
match ip address
match ip next-hop
match ip route-source
match metric
match route-type
match tag
route-map

set as-path
set automatic-tag
set community
set level
set local-preference
set metric
set metric-type
set next-hop
set origin
set weight

set weight

To specify the BGP weight for the routing table, use the **set weight** route-map configuration command. To delete an entry, use the **no** form of this command.

```
set weight weight
no set weight weight
```

Syntax Description

<i>weight</i>	Weight value. It can be an integer from 0 through 65535.
---------------	--

Default

The weight is not changed by the specified route map.

Command Mode

Route-map configuration

Usage Guidelines

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

The implemented weight is based on the first matched autonomous system path. Weights indicated when an autonomous system path is matched override the weights assigned by global **neighbor** commands. In other words, the weights assigned with the **match as-path** and **set weight** route-map commands override the weights assigned using the **neighbor weight** and **neighbor filter-list** commands.

Example

In the following example, the BGP weight for the routes matching the autonomous system path access list is set to 200:

```
route-map set-weight
  match as-path 10
  set weight 200
```

Related Commands

- match as-path**
- match community-list**
- match interface**
- match ip address**
- match ip next-hop**
- match ip route-source**
- match metric**
- match route-type**
- match tag**
- route-map**
- set as-path**
- set automatic-tag**
- set community**

set level
set local-preference
set metric
set metric-type
set next-hop
set origin
set tag

show ip bgp

To display entries in the BGP routing table, use the **show ip bgp** EXEC command.

show ip bgp [network] [network-mask] [longer-prefixes]

Syntax Description

<i>network</i>	(Optional) Network number, entered to display a particular network in the BGP routing table.
<i>network-mask</i>	(Optional) Displays all BGP routes matching the address/mask pair.
longer-prefixes	(Optional) Displays route and more specific routes.

Command Mode

EXEC

Sample Display

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

```
Router# show ip bgp

BGP table version is 716977, local router ID is 193.0.32.1
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

      Network          Next Hop            Metric LocPrf Weight Path
* i3.0.0.0          193.0.22.1        0       100      0 1800 1239 ?
* >i               193.0.16.1        0       100      0 1800 1239 ?
* i6.0.0.0          193.0.22.1        0       100      0 1800 690 568 ?
* >i               193.0.16.1        0       100      0 1800 690 568 ?
* i7.0.0.0          193.0.22.1        0       100      0 1800 701 35 ?
* >i               193.0.16.1        0       100      0 1800 701 35 ?
*                   198.92.72.24      0       100      0 1878 704 701 35 ?
* i8.0.0.0          193.0.22.1        0       100      0 1800 690 560 ?
* >i               193.0.16.1        0       100      0 1800 690 560 ?
*                   198.92.72.24      0       100      0 1878 704 701 560 ?
* i13.0.0.0          193.0.22.1        0       100      0 1800 690 200 ?
* >i               193.0.16.1        0       100      0 1800 690 200 ?
*                   198.92.72.24      0       100      0 1878 704 701 200 ?
* i15.0.0.0          193.0.22.1        0       100      0 1800 174 ?
* >i               193.0.16.1        0       100      0 1800 174 ?
* i16.0.0.0          193.0.22.1        0       100      0 1800 701 i
* >i               193.0.16.1        0       100      0 1800 701 i
*                   198.92.72.24      0       100      0 1878 704 701 i
```

Table 19-6 describes significant fields shown in the display.

Table 19-6 Show IP BGP Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.

Field	Description
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values:
s suppressed	Entry is suppressed.
* valid	Entry is valid.
> best	Entry is the best to use for that network.
i -internal	Entry learned via an internal BGP session.
Origin codes	Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values:
i - IGP	Entry originated from IGP and was advertised with a network router configuration command.
e - EGP	Entry originated from EGP.
? - incomplete	Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IP address of a network entity.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
Metric	If shown, this is the value of the interautonomous system metric. This is frequently not used.
LocPrf	Local preference value as set with the set local-preference route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

The following is sample output from the **show ip bgp** command when you specify **longer-prefixes**:

```
Router# show ip bgp 198.92.0.0 255.255.0.0 longer-prefixes
```

```
BGP table version is 1738, local router ID is 198.92.72.24
```

```
Status codes: s suppressed, * valid, > best, i - internal
```

```
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 198.92.0.0	198.92.72.30	8896	32768	?	
*	198.92.72.30		0	109 108	?
*> 198.92.1.0	198.92.72.30	8796	32768	?	
*	198.92.72.30		0	109 108	?
*> 198.92.11.0	198.92.72.30	42482	32768	?	
*	198.92.72.30		0	109 108	?
*> 198.92.14.0	198.92.72.30	8796	32768	?	
*	198.92.72.30		0	109 108	?
*> 198.92.15.0	198.92.72.30	8696	32768	?	
*	198.92.72.30		0	109 108	?
*> 198.92.16.0	198.92.72.30	1400	32768	?	
*	198.92.72.30		0	109 108	?
*> 198.92.17.0	198.92.72.30	1400	32768	?	
*	198.92.72.30		0	109 108	?
*> 198.92.18.0	198.92.72.30	8876	32768	?	
*	198.92.72.30		0	109 108	?
*> 198.92.19.0	198.92.72.30	8876	32768	?	
*	198.92.72.30		0	109 108	?

show ip bgp cidr-only

To display routes with nonnatural network masks (classless interdomain routing [CIDR]), use the **show ip bgp cidr-only** privileged EXEC command.

show ip bgp cidr-only

Syntax Description

This command has no arguments or keywords.

Command Mode

Privileged EXEC

Sample Display

The following is sample output from the **show ip bgp cidr-only** command:

```
Router# show ip bgp cidr-only

BGP table version is 220, local router ID is 198.92.73.131
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

      Network          Next Hop          Metric LocPrf Weight Path
* > 192.0.0.0/8      198.92.72.24      0 1878  ??
* > 198.92.0.0/16    198.92.72.30      0 108  ??
```

show ip bgp community

To display routes that belong to specified BGP communities, use the **show ip bgp community** EXEC command.

show ip bgp community *community-number* [exact]

Syntax Description

<i>community-number</i>	Valid value is community number in the range from 1 through 4294967200, internet , no-export , or no-advertise .
exact	(Optional) Displays only routes that have exactly the same specified communities.

Command Mode

EXEC

Sample Display

The following is sample output from the **show ip bgp community** command:

```
Router# show ip bgp community 10

BGP table version is 716977, local router ID is 193.0.32.1
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

      Network          Next Hop      Metric LocPrf Weight Path
* i3.0.0.0          193.0.22.1      0    100      0 1800 1239 ?
* >i               193.0.16.1      0    100      0 1800 1239 ?
* i6.0.0.0          193.0.22.1      0    100      0 1800 690 568 ?
* >i               193.0.16.1      0    100      0 1800 690 568 ?
* i7.0.0.0          193.0.22.1      0    100      0 1800 701 35 ?
* >i               193.0.16.1      0    100      0 1800 701 35 ?
*                   198.92.72.24      0          0 1878 704 701 35 ?
* i8.0.0.0          193.0.22.1      0    100      0 1800 690 560 ?
* >i               193.0.16.1      0    100      0 1800 690 560 ?
*                   198.92.72.24      0          0 1878 704 701 560 ?
* i13.0.0.0          193.0.22.1      0    100      0 1800 690 200 ?
* >i               193.0.16.1      0    100      0 1800 690 200 ?
*                   198.92.72.24      0          0 1878 704 701 200 ?
* i15.0.0.0          193.0.22.1      0    100      0 1800 174 ?
* >i               193.0.16.1      0    100      0 1800 174 ?
* i16.0.0.0          193.0.22.1      0    100      0 1800 701 i
* >i               193.0.16.1      0    100      0 1800 701 i
*                   198.92.72.24      0          0 1878 704 701 i
```

Table 19-7 describes significant fields shown in the display.

Table 19-7 Show IP BGP Community Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.

show ip bgp community

Field	Description
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values:
s suppressed	Entry is suppressed.
* valid	Entry is valid.
> best	Entry is the best to use for that network.
i -internal	Entry learned via an internal BGP session.
Origin codes	Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values:
i - IGP	Entry originated from IGP and was advertised with a network router configuration command.
e - EGP	Entry originated from EGP.
? - incomplete	Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IP address of a network entity.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
Metric	If shown, this is the value of the interautonomous system metric. This is frequently not used.
LocPrf	Local preference value as set with the set local-preference route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

show ip bgp community-list

To display routes that are permitted by the BGP community list, use the **show ip bgp community-list** EXEC command.

show ip bgp community-list *community-list-number* [exact]

Syntax Description

community-list-number Community list number in the range from 1 through 99.
exact (Optional) Displays only routes that have an exact match.

Command Mode

EXEC

Sample Display

The following is sample output of the **show ip bgp community-list** command:

```
Router# show ip bgp community-list 20

BGP table version is 716977, local router ID is 193.0.32.1
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

      Network          Next Hop            Metric LocPrf Weight Path
* i3.0.0.0          193.0.22.1        0      100      0 1800 1239 ?
* >i               193.0.16.1        0      100      0 1800 1239 ?
* i6.0.0.0          193.0.22.1        0      100      0 1800 690 568 ?
* >i               193.0.16.1        0      100      0 1800 690 568 ?
* i7.0.0.0          193.0.22.1        0      100      0 1800 701 35 ?
* >i               193.0.16.1        0      100      0 1800 701 35 ?
*                   198.92.72.24        0      100      0 1878 704 701 35 ?
* i8.0.0.0          193.0.22.1        0      100      0 1800 690 560 ?
* >i               193.0.16.1        0      100      0 1800 690 560 ?
*                   198.92.72.24        0      100      0 1878 704 701 560 ?
* i13.0.0.0          193.0.22.1        0      100      0 1800 690 200 ?
* >i               193.0.16.1        0      100      0 1800 690 200 ?
*                   198.92.72.24        0      100      0 1878 704 701 200 ?
* i15.0.0.0          193.0.22.1        0      100      0 1800 174 ?
* >i               193.0.16.1        0      100      0 1800 174 ?
* i16.0.0.0          193.0.22.1        0      100      0 1800 701 i
* >i               193.0.16.1        0      100      0 1800 701 i
*                   198.92.72.24        0      100      0 1878 704 701 i
```

Table 19-8 describes significant fields shown in the display.

Table 19-8 Show IP BGP Community List Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.

show ip bgp community-list

Field	Description
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values:
s suppressed	Entry is suppressed.
* valid	Entry is valid.
> best	Entry is the best to use for that network.
i -internal	Entry learned via an internal BGP session.
Origin codes	Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values:
i - IGP	Entry originated from IGP and was advertised with a network router configuration command.
e - EGP	Entry originated from EGP.
? - incomplete	Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IP address of a network entity.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
Metric	If shown, this is the value of the interautonomous system metric. This is frequently not used.
LocPrf	Local preference value as set with the set local-preference route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

show ip bgp filter-list

To display routes that conform to a specified filter list, use the **show ip bgp filter-list** privileged EXEC command.

show ip bgp filter-list *access-list-number*

Syntax Description

access-list-number Number of an autonomous system path access list. It can be a number from 1 through 199.

Command Mode

Privileged EXEC

Sample Display

The following is sample output from the **show ip bgp filter-list** command:

```
Router# show ip bgp filter-list 2

BGP table version is 1738, local router ID is 198.92.72.24
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

      Network          Next Hop            Metric LocPrf Weight Path
* 198.92.0.0        198.92.72.30          0 109 108 ?
* 198.92.1.0        198.92.72.30          0 109 108 ?
* 198.92.11.0       198.92.72.30          0 109 108 ?
* 198.92.14.0       198.92.72.30          0 109 108 ?
* 198.92.15.0       198.92.72.30          0 109 108 ?
* 198.92.16.0       198.92.72.30          0 109 108 ?
* 198.92.17.0       198.92.72.30          0 109 108 ?
* 198.92.18.0       198.92.72.30          0 109 108 ?
* 198.92.19.0       198.92.72.30          0 109 108 ?
* 198.92.24.0       198.92.72.30          0 109 108 ?
* 198.92.29.0       198.92.72.30          0 109 108 ?
* 198.92.30.0       198.92.72.30          0 109 108 ?
* 198.92.33.0       198.92.72.30          0 109 108 ?
* 198.92.35.0       198.92.72.30          0 109 108 ?
* 198.92.36.0       198.92.72.30          0 109 108 ?
* 198.92.37.0       198.92.72.30          0 109 108 ?
* 198.92.38.0       198.92.72.30          0 109 108 ?
* 198.92.39.0       198.92.72.30          0 109 108 ?
```

show ip bgp inconsistent-as

To display routes with inconsistent originating autonomous systems, use the **show ip bgp inconsistent-as** privileged EXEC command.

show ip bgp inconsistent-as

Syntax Description

This command has no arguments or keywords.

Command Mode

Privileged EXEC

Sample Display

The following is sample output from the **show ip bgp inconsistent-as** command:

```
Router# show ip bgp inconsistent-as
BGP table version is 87, local router ID is 172.19.82.53
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

      Network          Next Hop          Metric LocPrf Weight Path
*  11.0.0.0        171.69.232.55      0        0 300 88 90 99 ?
* >               171.69.232.52      2222      0 400 ?
*  171.69.0.0      171.69.232.55      0        0 300 90 99 88 200 ?
* >               171.69.232.52      2222      0 400 ?
*  200.200.199.0   171.69.232.55      0        0 300 88 90 99 ?
* >               171.69.232.52      2222      0 400 ?
```

show ip bgp neighbors

To display information about the TCP and BGP connections to neighbors, use the **show ip bgp neighbors** EXEC command.

show ip bgp neighbors [address [routes | paths]]

Syntax Description

address	(Optional) Address of the neighbor whose routes you have learned from.
routes	(Optional) If you specify an address, displays routes from the specified neighbor.
paths	(Optional) If you specify an address, displays autonomous system paths of the routes received from the specified neighbor.

Command Mode

EXEC

Sample Displays

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

```
Router# show ip bgp neighbors

BGP neighbor is 131.108.6.68, remote AS 10, external link
BGP version 3, remote router ID 131.108.6.68
BGP state = Established, table version = 22, up for 0:00:13
Last read 0:00:12, hold time is 180, keepalive interval is 60 seconds
Received 24 messages, 0 notifications
Sent 28 messages, 4 notifications
Connections established 1; dropped 0
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Local host: 131.108.6.69, 12288  Foreign host: 131.108.6.68, 179

Enqueued packets for retransmit: 0, input: 0, saved: 0

Event Timers (current time is 835828):
Timer:      Retrans   TimeWait   AckHold   SendWnd   KeepAlive
Starts:      20        0          18        0          0
Wakeups:     1          0          2          0          0
Next:        0          0          0          0          0

iss:      60876  snduna:      62649  sndnxt:      62649  sndwnd:    1872
irs:    95187024  rcvnxt:  95188733  rcvwnd:    1969  delrcvwnd:  271

SRTT: 364 ms, RTTO: 1691 ms, RTV: 481 ms, KRTT: 0 ms
minRTT: 4 ms, maxRTT: 340 ms, ACK hold: 300 ms
Flags: higher precedence

Datagrams (max data segment is 1450 bytes):
Rcvd: 36 (out of order: 0), with data: 18, total data bytes: 1708
Sent: 40 (retransmit: 1), with data: 36, total data bytes: 1817
```

Table 19-9 describes the fields shown in the display.

Table 19-9 Show IP BGP Neighbors Field Descriptions

Field	Description
BGP neighbor	Lists the IP address of the BGP neighbor and its autonomous system number. If the neighbor is in the same autonomous system as the router, then the link between them is internal. Otherwise, it is considered external.
BGP version	Specifies that the BGP version being used to communicate with the remote router is BGP version 3; the neighbor's router ID (an IP address) is also specified.
BGP state	Indicates the internal state of this BGP connection.
table version	Indicates that the neighbor has been updated with this version of the primary BGP routing table.
up time	Indicates the amount of time that the underlying TCP connection has been in existence.
Last read	Time that BGP last read a message from this neighbor.
hold time	Maximum amount of time that can elapse between messages from the peer.
keepalive interval	Time period between sending keepalive packets, which help ensure that the TCP connection is up.
Received	Number of received messages indicates the number of total BGP messages received from this peer, including keepalives. The number of notifications is the number of error messages received from the peer.
Sent	The number of sent messages indicates the total number of BGP messages that have been sent to this peer, including keepalives. The number of notifications is the number of error messages that we have sent to this peer.
Connections established	The number of connections established is a count of the number of times that we have established a TCP connection and the two peers have agreed to speak BGP with each other. The number of dropped connections is the number of times that a good connection has failed or been taken down.

The remainder of the display describes the status of the underlying TCP connection.

The following is sample output from the **show ip bgp neighbors** command when you specify the **routes** keyword:

```
Router# show ip bgp neighbors 198.41.177.210 routes
BGP table version is 212136, local router ID is 131.108.5.225
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
Network          Next Hop          Metric LocPrf Weight Path
*> 163.179.0.0   192.41.177.210          100 2551 i
*  192.203.50.0  192.41.177.210          100 2551 ?
*> 199.183.0.0/16 192.41.177.210          100 2551 i
```

Table 19-10 describes the fields shown in the display.

Table 19-10 Show IP BGP Neighbors Routes Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values:
s suppressed	Entry is suppressed.
* valid	Entry is valid.
> best	Entry is the best to use for that network.
i -internal	Entry learned via an internal BGP session.
Origin codes	Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values:
i - IGP	Entry originated from IGP and was advertised with a network router configuration command.
e - EGP	Entry originated from EGP.
? - incomplete	Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IP address of a network entity.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
Metric	If shown, this is the value of the interautonomous system metric. This is frequently not used.
LocPrf	Local preference value as set with the set local-preference route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

show ip bgp paths

To display all the BGP paths in the database, use the **show ip bgp paths** EXEC command.

show ip bgp paths

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

Sample Display

The following is sample output from the **show ip bgp paths** command:

```
Router# show ip bgp paths
Address      Hash  Refcount Metric  Path
0x297A9C      0      2        0  i
0x30BF84      1      0        0  702 701 ?
0x2F7BC8      2      235      0  ?
0x2FA1D8      3      0        0  702 701 i
```

Table 19-11 describes significant fields shown in the display.

Table 19-11 Show IP BGP Paths Field Descriptions

Field	Description
Address	Internal address where the path is stored.
Hash	Hash bucket where path is stored.
Refcount	Number of routes using that path.
Metric	The multiple exit discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.)
Path	The AS_PATH for that route, followed by the origin code for that route.

show ip bgp peer-group

To display information about BGP peer groups, use the **show ip bgp peer-group** EXEC command.

show ip bgp peer-group [tag] [summary]

Syntax Description

tag	(Optional) Displays information about that specific peer group.
summary	(Optional) Displays a summary of the status of all the members of a peer group.

Command Mode

EXEC

Sample Display

The following is sample output from the **show ip bgp peer-group** command:

```
Router# show ip bgp peer-group0 internal
BGP neighbor is internal, peer-group leader
  BGP version 4
  Minimum time between advertisement runs is 5 seconds
  Incoming update AS path filter list is 2
  Outgoing update AS path filter list is 1
  Route map for outgoing advertisements is set-med
```

show ip bgp regexp

To display routes matching the regular expression, use the **show ip bgp regexp** privileged EXEC command.

show ip bgp regexp *regular-expression*

Syntax Description

<i>regular-expression</i>	Regular expression to match the BGP autonomous system paths.
---------------------------	--

Command Mode

Privileged EXEC

Sample Display

```
Router# show ip bgp regexp 108$  
  
BGP table version is 1738, local router ID is 198.92.72.24  
Status codes: s suppressed, * valid, > best, i - internal  
Origin codes: i - IGP, e - EGP, ? - incomplete  
  
Network          Next Hop          Metric LocPrf Weight Path  
* 198.92.0.0      198.92.72.30      0 109 108 ?  
* 198.92.1.0      198.92.72.30      0 109 108 ?  
* 198.92.11.0     198.92.72.30      0 109 108 ?  
* 198.92.14.0     198.92.72.30      0 109 108 ?  
* 198.92.15.0     198.92.72.30      0 109 108 ?  
* 198.92.16.0     198.92.72.30      0 109 108 ?  
* 198.92.17.0     198.92.72.30      0 109 108 ?  
* 198.92.18.0     198.92.72.30      0 109 108 ?  
* 198.92.19.0     198.92.72.30      0 109 108 ?  
* 198.92.24.0     198.92.72.30      0 109 108 ?  
* 198.92.29.0     198.92.72.30      0 109 108 ?  
* 198.92.30.0     198.92.72.30      0 109 108 ?  
* 198.92.33.0     198.92.72.30      0 109 108 ?  
* 198.92.35.0     198.92.72.30      0 109 108 ?  
* 198.92.36.0     198.92.72.30      0 109 108 ?  
* 198.92.37.0     198.92.72.30      0 109 108 ?  
* 198.92.38.0     198.92.72.30      0 109 108 ?  
* 198.92.39.0     198.92.72.30      0 109 108 ?
```

show ip bgp summary

To display the status of all BGP connections, use the **show ip bgp summary** EXEC command.

show ip bgp summary

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

Sample Display

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

```
Router# show ip bgp summary

BGP table version is 717029, main routing table version 717029
19073 network entries (37544 paths) using 3542756 bytes of memory
691 BGP path attribute entries using 57200 bytes of memory

Neighbor      V   AS MsgRcvd MsgSent    TblVer  InQ  OutQ Up/Down  State
193.0.16.1    4   1755  32642   2973    717029  0    0   1:27:11
193.0.17.1    4   1755  4790    2973    717029  0    0   1:27:51
193.0.18.1    4   1755  7722    3024    717029  0    0   1:28:13
193.0.19.1    4   1755  0        0        717029  0    0   0 2d02    Active
193.0.20.1    4   1755  3673    3049    717029  0    0   0 2:50:10
193.0.21.1    4   1755  3741    3048    717029  0    0   0 12:24:43
193.0.22.1    4   1755  33129   3051    717029  0    0   0 12:24:48
193.0.23.1    4   1755  0        0        717029  0    0   0 2d02    Active
193.0.24.1    4   1755  0        0        717029  0    0   0 2d02    Active
193.0.25.1    4   1755  0        0        717029  0    0   0 2d02    Active
193.0.26.1    4   1755  0        0        717029  0    0   0 2d02    Active
193.0.27.1    4   1755  4269    3049    717029  0    0   0 12:39:33
193.0.28.1    4   1755  3037    3050    717029  0    0   0 2:08:15
198.92.72.24  4   1878  11635   13300   717028  0    0   0 0:50:39
```

Table 19-12 describes significant fields shown in the display.

Table 19-12 Show IP BGP Summary Field Descriptions

Field	Description
BGP table version	Internal version number of BGP database.
main routing table version	Indicates last version of BGP database that was injected into main routing table.
Neighbor	IP address of a neighbor.
V	Indicates BGP version number spoken to that neighbor.
MsgRcvd	BGP messages received from that neighbor.
MsgSent	BGP messages sent to that neighbor.
TblVer	Last version of the BGP database that was sent to that neighbor.
InQ	Number of messages from that neighbor waiting to be processed.

show ip bgp summary

Field	Description
OutQ	Number of messages waiting to be sent to that neighbor.
Update/State	The length of time that the BGP session has been in state Established, or the current state if it is not Established.

show ip dvmrp route

To display the contents of the DVMRP routing table, use the **show ip dvmrp route** EXEC command.

show ip dvmrp route [ip-address]

Syntax Description

ip-address (Optional) IP address or name of an entry in the DVMRP routing table.

Command Mode

EXEC

Sample Display

The following is sample output of the **show ip dvmrp route** command:

```
Router# show ip dvmrp route

DVMRP Routing Table - 3 entries
13.0.32.0/22 [0/11]
  via 192.88.195.10, Tunnell, uptime 3:50:24, expires 0:02:24
13.0.52.0/22 [0/9]
  via 192.88.195.10, Tunnell, uptime 0:59:14, expires 0:02:24
13.1.68.0/22 [0/8]
  via 192.88.195.10, Tunnell, uptime 3:50:24, expires 0:02:24
```

Table 19-13 describes the fields shown in the display

Table 19-13 Show IP DVMRP Route Field Descriptions

Field	Description
3 entries	Number of entries in the DVMRP routing table.
13.0.32.0/22	Source network.
[0/11]	Administrative distance/reliability.
via 192.88.195.10	Next-hop router to the source network.
Tunnell	Interface to the source network.
uptime	How long in hours, minutes, and seconds that the route has been in the DVMRP routing table.
expires	How long in hours, minutes, and seconds until the entry is removed from the DVMRP routing table.

Related Command

ip dvmrp accept-filter

show ip egp

To display statistics about EGP connections and neighbors, use the **show ip egp** EXEC command.

show ip egp

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

Sample Display

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

```
Router# show ip egp

  Local autonomous system is 109
  EGP Neighbor FAS/LAS State    SndSeq RcvSeq Hello Poll j/k Flags
  10.3.0.27      1/109 IDLE      625   61323    60   180    0 Perm, Act
  * 10.2.0.37    1/109 UP       12:29   250   14992    60   180    3 Perm, Act
  * 10.7.0.63    1/109 UP       1d19    876   10188    60   180    4 Perm, Pass
```

Table 19-14 describes the fields shown in the display.

Table 19-14 Show IP EGP Field Descriptions

Field	Description
EGP Neighbor	Address of the EGP neighbor.
FAS	Foreign autonomous system number.
LAS	Local autonomous system number.
State	State of the connection between peers.
SndSeq	Send sequence number.
RcvSeq	Receive sequence number.
Hello	Interval between Hello/I-Heard-You packets.
Poll	Interval between Poll/Update packets.
j/k	Measure of reachability; 4 is perfect.
Flags	Perm—Permanent. Temp—Temporary (neighbor will be removed). Act—Active, controlling the connection. Pass—Passive, neighbor controls the connection.

show ip eigrp neighbors

To display the neighbors discovered by Enhanced IGRP, use the **show ip eigrp neighbors** EXEC command.

show ip eigrp neighbors [type number]

Syntax Description

type (Optional) Interface type.
number (Optional) Interface number.

Command Mode

EXEC

Usage Guidelines

Use the **show ip eigrp neighbors** command to determine when neighbors become active and inactive. It is also useful for debugging certain types of transport problems.

Sample Display

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

```
Router# show ip eigrp neighbors

IP-EIGRP Neighbors for process 77
Address           Interface      Holdtime Uptime   Q      Seq    SRTT   RTO
                  (secs)      (h:m:s)  Count   Num   (ms)   (ms)
160.89.81.28     Ethernet1    13        0:00:41  0      11     4      20
160.89.80.28     Ethernet0    14        0:02:01  0      10     12     24
160.89.80.31     Ethernet0    12        0:02:02  0      4      5      20
```

Table 19-15 explains the fields in the output.

Table 19-15 Show IP EIGRP Neighbors Field Descriptions

Field	Description
process 77	Autonomous system number specified in the router configuration command.
Address	IP address of the enhanced IGRP peer.
Interface	Interface on which the router is receiving hello packets from the peer.
Holdtime	Length of time, in seconds, that the router will wait to hear from the peer before declaring it down. If the peer is using the default hold time, this number will be less than 15. If the peer configures a nondefault hold time, it will be reflected here.
Uptime	Elapsed time, in hours, minutes, and seconds, since the local router first heard from this neighbor.
Q Count	Number of Enhanced IGRP packets (Update, Query, and Reply) that the router is waiting to send.
Seq Num	Sequence number of the last update, query, or reply packet that was received from this neighbor.

show ip eigrp neighbors

Field	Description
SRTT	Smooth round-trip time. This is the number of milliseconds it takes for an Enhanced IGRP packet to be sent to this neighbor and for the local router to receive an acknowledgment of that packet.
RTO	Retransmission timeout, in milliseconds. This is the amount of time the router waits before retransmitting a packet from the retransmission queue to a neighbor.

show ip eigrp topology

To display the Enhanced IGRP topology table, use the **show ip eigrp topology** EXEC command.

show ip eigrp topology [autonomous-system-number | [[ip-address] mask]]

Syntax Description

<i>autonomous-system-number</i>	(Optional) Autonomous system number.
<i>ip-address</i>	(Optional) IP address. When specified with a mask, a detailed description of the entry is provided.
<i>mask</i>	(Optional) Subnet mask.

Command Mode

EXEC

Usage Guidelines

Use the **show ip eigrp topology** command to determine DUAL states and to debug possible DUAL problems.

Sample Display

The following is sample output from the **show ip eigrp topology** command:

```
Router# show ip eigrp topology
IP-EIGRP Topology Table for process 77
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 160.89.90.0 255.255.255.0, 2 successors, FD is 0
      via 160.89.80.28 (46251776/46226176), Ethernet0
      via 160.89.81.28 (46251776/46226176), Ethernet1
      via 160.89.80.31 (46277376/46251776), Ethernet0
P 160.89.81.0 255.255.255.0, 1 successors, FD is 307200
      via Connected, Ethernet1
      via 160.89.81.28 (307200/281600), Ethernet1
      via 160.89.80.28 (307200/281600), Ethernet0
      via 160.89.80.31 (332800/307200), Ethernet0
```

Table 19-16 explains the fields in the output.

Table 19-16 Show IP EIGRP Topology Field Descriptions

Field	Description
Codes	State of this topology table entry. Passive and Active refer to the Enhanced IGRP state with respect to this destination; Update, Query, and Reply refer to the type of packet that is being sent.
P – Passive	No Enhanced IGRP computations are being performed for this destination.
A – Active	Enhanced IGRP computations are being performed for this destination.

show ip eigrp topology

Field	Description
U – Update	Indicates that an update packet was sent to this destination.
Q – Query	Indicates that a query packet was sent to this destination.
R – Reply	Indicates that a reply packet was sent to this destination.
r – Reply status	Flag that is set when after the router has sent a query and is waiting for a reply.
160.89.90.0 and so on	Destination IP network number.
255.255.255.0	Destination subnet mask.
successors	Number of successors. This number corresponds to the number of next hops in the IP routing table.
FD	Feasible distance. This value is used in the feasibility condition check. If the neighbor's reported distance (the metric after the slash) is less than the feasible distance, the feasibility condition is met and that path is a feasible successor. Once the router determines it has a feasible successor, it does not have to send a query for that destination.
replies	Number of replies that are still outstanding (have not been received) with respect to this destination. This information appears only when the destination is in Active state.
state	Exact Enhanced IGRP state that this destination is in. It can be the number 0, 1, 2, or 3. This information appears only when the destination is Active.
via	IP address of the peer who told the router about this destination. The first N of these entries, where N is the number of successors, are the current successors. The remaining entries on the list are feasible successors.
(46251776/46226176)	The first number is the Enhanced IGRP metric that represents the cost to the destination. The second number is the Enhanced IGRP metric that this peer advertised.
Ethernet0	Interface from which this information was learned.

show ip eigrp traffic

To display the number of Enhanced IGRP packets sent and received, use the **show ip eigrp traffic** EXEC command.

show ip eigrp traffic [autonomous-system-number]

Syntax Description

autonomous-system-number (Optional) Autonomous system number.

Command Mode

EXEC

Sample Display

The following is sample output from the **show ip eigrp traffic** command:

```
Router# show ip eigrp traffic

IP-EIGRP Traffic Statistics for process 77
    Hellos sent/received: 218/205
    Updates sent/received: 7/23
    Queries sent/received: 2/0
    Replies sent/received: 0/2
    Acks sent/received: 21/14
```

Table 19-17 describes the fields that might be shown in the display.

Table 19-17 Show IP EIGRP Traffic Field Descriptions

Field	Description
process 77	Autonomous system number specified in the ip router command.
Hellos sent/received	Number of hello packets that were sent and received.
Updates sent/received	Number of update packets that were sent and received.
Queries sent/received	Number of query packets that were sent and received.
Replies sent/received	Number of reply packets that were sent and received.
Acks sent/received	Number of acknowledgment packets that were sent and received.

show ip igmp groups

To display the multicast groups that are directly connected to the router and that were learned via IGMP, use the **show ip igmp groups** EXEC command.

show ip igmp groups [*group-name* | *group-address* | *type number*]

Syntax Description

<i>group-name</i>	(Optional) Name of the multicast group, as defined in the DNS hosts table.
<i>group-address</i>	(Optional) Address of the multicast group. This is a multicast IP address in four-part dotted notation.
<i>type</i>	(Optional) Interface type.
<i>number</i>	(Optional) Interface number.

Command Mode

EXEC

Usage Guidelines

If you omit all optional arguments, the **show ip igmp groups** command displays by group address and interface type and number all directly connected multicast groups.

Sample Display

The following is sample output from the **show ip igmp groups** command:

```
Router# show ip igmp groups

IGMP Connected Group Membership
Group Address      Interface      Uptime      Expires      Last Reporter
224.0.255.1        Ethernet0     18:51:41    0:02:15     198.92.37.192
224.2.226.60       Ethernet0     1:51:31     0:02:17     198.92.37.192
224.2.127.255     Ethernet0     18:51:45    0:02:17     198.92.37.192
226.2.2.2          Ethernet1     18:51:47    never       0.0.0.0
224.2.0.1          Ethernet0     18:51:43    0:02:14     198.92.37.192
225.2.2.2          Ethernet0     18:51:43    0:02:21     198.92.37.33
225.2.2.2          Ethernet1     18:51:47    never       0.0.0.0
225.2.2.4          Ethernet0     18:18:02    0:02:20     198.92.37.192
225.2.2.4          Ethernet1     18:23:32    0:02:55     198.92.36.128
```

Table 19-18 describes the fields shown in the display.

Table 19-18 Show IP IGMP Groups Field Descriptions

Field	Description
Group address	Address of the multicast group.
Interface	Interface through which the group is reachable.
Uptime	How long in hours, minutes, and seconds this multicast group has been known.
Expires	How long in hours, minutes, and seconds until the entry is removed from the IGMP groups table.
Last Reporter	Last host to report being a member of the multicast group.

Related Command**ip igmp query-interval**

show ip igmp interface

To display multicast-related information about an interface, use the **show ip igmp interface** EXEC command.

show ip igmp interface [*type number*]

Syntax Description

<i>type</i>	(Optional) Interface type.
<i>number</i>	(Optional) Interface number.

Command Mode

EXEC

Usage Guidelines

If you omit the optional arguments, the **show ip igmp interface** command displays information about all interfaces.

This command also displays information about dynamically learned DVMRP routers on the interface.

Sample Display

The following is sample output from the **show ip igmp interface** command:

```
Router# show ip igmp interface

Ethernet0 is up, line protocol is up
  Internet address is 198.92.37.6, subnet mask is 255.255.255.0
  IGMP is enabled on interface
  IGMP query interval is 60 seconds
  Inbound IGMP access group is not set
  Multicast routing is enabled on interface
  Multicast TTL threshold is 0
  Multicast designated router (DR) is 198.92.37.33
  No multicast groups joined
Ethernet1 is up, line protocol is up
  Internet address is 198.92.36.129, subnet mask is 255.255.255.0
  IGMP is enabled on interface
  IGMP query interval is 60 seconds
  Inbound IGMP access group is not set
  Multicast routing is enabled on interface
  Multicast TTL threshold is 0
  Multicast designated router (DR) is 198.92.36.131
  Multicast groups joined: 225.2.2.2 226.2.2.2
Tunnel0 is up, line protocol is up
  Internet address is 10.1.37.2, subnet mask is 255.255.0.0
  IGMP is enabled on interface
  IGMP query interval is 60 seconds
  Inbound IGMP access group is not set
  Multicast routing is enabled on interface
  Multicast TTL threshold is 0
  No multicast groups joined
```

Table 19-19 describes the fields shown in the display.

Table 19-19 Show IP IGMP Interface Field Descriptions

Field	Description
Ethernet0 is up, line protocol is up	Interface type, number, and status.
Internet address is... subnet mask is...	Internet address of the interface and subnet mask being applied to the interface, as specified with the ip address command.
IGMP is enabled on interface	Indicates whether IGMP has been enabled on the interface with the ip pim command.
IGMP query interval is 60 seconds	Interval at which the router sends PIM router-query messages, as specified with the ip igmp query-interval command.
Inbound IGMP access group is not set	Indicates whether an IGMP access group has been configured with the ip igmp access-group command.
Multicast routing is enabled on interface	Indicates whether multicast routing has been enabled on the interface with the ip pim command.
Multicast TTL threshold is 0	Packet time-to-threshold, as specified with the ip multicast ttl-threshold command.
Multicast designated router (DR) is...	IP address of the designated router for this LAN segment (subnet).
Multicast groups joined: No multicast groups joined	Indicates whether this interface is a member of any multicast groups and, if so, lists the IP addresses of the groups.

Related Commands

ip address
ip igmp access-group
ip igmp query-interval
ip multicast ttl-threshold
ip pim

show ip irdp

To display IRDP values, use the **show ip irdp** EXEC command.

show ip irdp

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

Sample Display

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

```
Router# show ip irdp

Ethernet 0 has router discovery enabled

Advertisements will occur between every 450 and 600 seconds.
Advertisements are valid for 1800 seconds.
Default preference will be 100.
--More--
Serial 0 has router discovery disabled
--More--
Ethernet 1 has router discovery disabled
```

As the display shows, **show ip irdp** output indicates whether router discovery has been configured for each router interface, and lists the values of router discovery configurables for those interfaces on which router discovery has been enabled. Explanations for the less self-evident lines of output in the display follow.

Advertisements will occur between every 450 and 600 seconds.

Indicates the configured minimum and maximum advertising interval for the interface.

Advertisements are valid for 1800 seconds.

Indicates the configured holdtime values for the interface.

Default preference will be 100.

Indicates the configured (or in this case default) preference value for the interface.

show ip mcache

To display the contents of the IP fast switching cache, use the **show ip mcache** EXEC command.

show ip mcache [group [source]]

Syntax Description

group (Optional) Displays the fast switching cache for the single group. The *group* argument can be either a Class D IP address or a DNS name.

source (Optional) If *source* is also specified, displays a single multicast cache entry. The *source* argument can be either a unicast IP address or a DNS name.

Command Mode

EXEC

Sample Display

The following is sample output from the **show ip mcache** command. This entry shows a specific source (wrn-source 204.62.246.73) sending to the World Radio Network group (224.2.143.24).

```
Router> show ip mcache wrn wrn-source
IP Multicast Fast-Switching Cache
(204.62.246.73/32, 224.2.143.24), Fddi0, Last used: 00:00:00
  Ethernet0      MAC Header: 01005E028F1800000C1883D30800
  Ethernet1      MAC Header: 01005E028F1800000C1883D60800
  Ethernet2      MAC Header: 01005E028F1800000C1883D40800
  Ethernet3      MAC Header: 01005E028F1800000C1883D70800
```

Table 19-20 describes the significant fields in the display.

Table 19-20 Show IP Mcache Field Descriptions

Field	Description
204.62.246.73	Source address.
224.2.143.24	Destination address.
Fddi0	Incoming or expected interface the packet should be received on.
Last used:	Latest time the entry was accessed for a packet that was successfully fast switched. The word “Semi-fast” indicates that the first part of the outgoing interface list is fast switched and the rest of the list is process level switched.
Ethernet0	Outgoing interface list and respective MAC header that is used when rewriting the packet for output. If the interface is a tunnel, the MAC header will show the real next hop MAC header and then in parentheses the real interface name.
MAC Header:	

show ip mroute

To display the contents of the IP multicast routing table, use the **show ip mroute** EXEC command.

show ip mroute [group] [source] [summary] [count]

Syntax Description

group	(Optional) IP address or name of the multicast group as defined in the DNS hosts table.
source	(Optional) IP address or name of a multicast source.
summary	(Optional) Displays a one-line, abbreviated summary of each entry in the IP multicast routing table.
count	(Optional) Displays statistics about the group and source, including number of packets, packets per second, average packet size, and bits per second.

Command Mode

EXEC

Usage Guidelines

If you omit all optional arguments and keywords, the **show ip mroute** command displays all entries in the IP multicast routing table.

The router populates the multicast routing table by creating source, group (S,G) entries from star, group (*,G) entries. The star refers to all source addresses, the “S” refers to a single source address, and the “G” is the destination multicast group address. In creating (S,G) entries, the router uses the best path to that destination group found in the unicast routing table (that is, via Reverse Path Forwarding [RPF]).

Sample Displays

The following is sample output from the **show ip mroute** command for a router operating in dense mode. This command displays the contents of the IP multicast routing table for the multicast group named cbone-audio.

```
Router> show ip mroute cbone-audio

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, C - Connected, L - Local, P - Pruned
      R - RP-bit set, F - Register flag, T - SPT-bit set
Timers: Uptime/Expires
Interface state: Interface, Next-Hop, State/Mode

(*, 224.0.255.1), uptime 0:57:31, expires 0:02:59, RP is 0.0.0.0, flags: DC
  Incoming interface: Null, RPF neighbor 0.0.0.0, Dvmrp
  Outgoing interface list:
    Ethernet0, Forward/Dense, 0:57:31/0:02:52
    Tunnel0, Forward/Dense, 0:56:55/0:01:28

(198.92.37.100/32, 224.0.255.1), uptime 20:20:00, expires 0:02:55, flags: C
  Incoming interface: Tunnel0, RPF neighbor 10.20.37.33, Dvmrp
```

```
Outgoing interface list:
  Ethernet0, Forward/Dense, 20:20:00/0:02:52
```

The following is sample output from the **show ip mroute** command for a router operating in sparse mode:

```
Router# show ip mroute

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, C - Connected, L - Local, P - Pruned
      R - RP-bit set, F - Register flag, T - SPT-bit set
Timers: Uptime/Expires
Interface state: Interface, Next-Hop, State/Mode

(*, 224.0.255.3), uptime 5:29:15, RP is 198.92.37.2, flags: SC
  Incoming interface: Tunnel0, RPF neighbor 10.3.35.1, Dvmrp
  Outgoing interface list:
    Ethernet0, Forward/Sparse, 5:29:15/0:02:57

(198.92.46.0/24, 224.0.255.3), uptime 5:29:15, expires 0:02:59, flags: C
  Incoming interface: Tunnel0, RPF neighbor 10.3.35.1
  Outgoing interface list:
    Ethernet0, Forward/Sparse, 5:29:15/0:02:57
```

Table 19-21 explains the fields shown in the displays.

Table 19-21 Show IP Mroute Field Descriptions

Field	Description
Flags:	Provides information about the entry.
D - Dense	Entry is operating in dense mode.
S - Sparse	Entry is operating in sparse mode.
C - Connected	A member of the multicast group is present on the directly connected interface.
L - Local	The router itself is a member of the multicast group.
P - Pruned	Route has been pruned. The router keeps this information in case a downstream member wants to join the source.
R - Rp-bit set	Indicates that the (S,G) entry is pointing towards the RP. This is typically prune state along the shared tree for a particular source.
F - Register flag	Indicates that the router is Registering for a multicast source.
T - SPT-bit set	Indicates that packets have been received on the shortest path source tree.
(* , 224.0.255.1)	Entry in the IP multicast routing table. The entry consists of the IP address of the source router followed by IP address of the multicast group. An asterisk (*) in place of the source router indicates all sources.
(198.92.37.100/32, 224.0.255.1)	Entries in the first format are referred to as (*,G,) or “star comma G,” entries. Entries in the second format are referred to as (S,G) or (“S comma G”) entries. (*,G) entries are used to build (S,G) entries.
uptime	How long in hours, minutes, and seconds the entry has been in the IP multicast routing table.
expires	How long in hours, minutes, and seconds until the entry will be removed from the IP multicast routing table on the outgoing interface.

Field	Description
RP	Address of the rendezvous point (RP) router. For routers operating in sparse mode, this address is always 0.0.0.0.
flags:	Information about the entry.
Incoming interface:	Expected interface for a multicast packet from the source. If the packet is not received on this interface, it is discarded.
RPF neighbor	IP address of the upstream router to the source. “Tunneling” indicates that this router is sending data to the RP encapsulated in Register packets. The hexadecimal number in parentheses indicates which RP we are registering to. Each bit indicates a different RP if multiple RPs per group are used.
Dvmrp or Mroute	Indicates if the RPF information is obtained from the DVMRP routing table or the static mroutes configuration.
Outgoing interface list:	Interfaces through which packets will be forwarded. When the interface has ip pim nbma-mode , the IP address of the PIM neighbor is also displayed.
Ethernet0	Name and number of the outgoing interface.
Forward/Dense	Indicates that packets will be forwarded on the interface if there are no restrictions due to access lists or TTL threshold. Following the slash, mode in which the interface is operating (dense or sparse).
time/time	How long in hours, minutes, and seconds the entry has been in the IP multicast routing table. Following the slash, how long in hours, minutes, and seconds until the entry will be removed from the IP multicast routing table.

Related Command

ip igmp query-interval

show ip ospf

To display general information about OSPF routing processes, use the **show ip ospf** EXEC command.

show ip ospf [process-id]

Syntax Description

process-id (Optional) Process ID. If this argument is included, only information for the specified routing process is included.

Command Mode

EXEC

Sample Display

The following is sample output from the **show ip ospf** command when entered without a specific OSPF process ID:

```
Router# show ip ospf

Routing Process "ospf 201" with ID 192.42.110.200
Supports only single TOS(TOS0) route
It is an area border and autonomous system boundary router
Summary Link update interval is 0:30:00 and the update due in 0:16:26
External Link update interval is 0:30:00 and the update due in 0:16:27
Redistributing External Routes from,
    igrp 200 with metric mapped to 2, includes subnets in redistribution
    rip with metric mapped to 2
    igrp 2 with metric mapped to 100
    igrp 32 with metric mapped to 1
Number of areas in this router is 3
Area 192.42.110.0
    Number of interfaces in this area is 1
    Area has simple password authentication
    SPF algorithm executed 6 times
    Area ranges are
    Link State Update Interval is 0:30:00 and due in 0:16:55
    Link State Age Interval is 0:20:00 and due in 0:06:55
```

Table 19-22 describes significant fields shown in the display.

Table 19-22 Show IP OSPF Field Descriptions

Field	Description
Routing process “ospf 201” with ID 192.42.110.200	Process ID and OSPF router ID.
Type of Service	Number of Types of Service supported (Type 0 only).
Type of OSPF Router	Possible types are internal, area border, or autonomous system boundary.
Summary Link update interval	Specify summary update interval in hours:minutes:seconds, and time to next update.

show ip ospf

Field	Description
External Link update interval	Specify external update interval in hours:minutes:seconds, and time to next update.
Redistributing External Routes from	Lists of redistributed routes, by protocol.
Number of areas	Number of areas in router, area addresses, and so on.
Link State Update Interval	Specify router and network link state update interval in hours:minutes:seconds, and time to next update.
Link State Age Interval	Specify max-aged update deletion interval and time until next database cleanup in hours:minutes:seconds.

show ip ospf border-routers

To display the internal OSPF routing table entries to an Area Border Router (ABR) and Autonomous System Boundary Router (ASBR), use the **show ip ospf border-routers** privileged EXEC command.

show ip ospf border-routers

Syntax Description

This command has no arguments or keywords.

Command Mode

Privileged EXEC

Sample Display

The following is sample output from the **show ip ospf border-routers** command:

```
Router# show ip ospf border-routers

OSPF Process 109 internal Routing Table

      Destination      Next Hop      Cost      Type      Rte Type Area      SPF No
      160.89.97.53    144.144.1.53   10        ABR      INTRA      0.0.0.3      3
      160.89.103.51   160.89.96.51   10        ABR      INTRA      0.0.0.3      3
      160.89.103.52   160.89.96.51   20        ASBR     INTER      0.0.0.3      3
      160.89.103.52   144.144.1.53   22        ASBR     INTER      0.0.0.3      3
```

Table 19-23 describes the fields shown in the display.

Table 19-23 Show IP OSPF Border-routers Field Descriptions

Field	Description
Destination	Destination's router ID.
Next Hop	Next hop toward the destination.
Cost	Cost of using this route.
Type	The router type of the destination; it is either an Area Border Router (ABR) or Autonomous System Boundary Router (ASBR) or both.
Rte Type	The type of this route, it is either an intra-area or interarea route.
Area	The area ID of the area that this route is learned from.
SPF No	The internal number of SPF calculation that installs this route.

show ip ospf database

Use the **show ip ospf database** EXEC command to display lists of information related to the OSPF database for a specific router. The various forms of this command deliver information about different OSPF link state advertisements.

```
show ip ospf [process-id area-id] database
show ip ospf [process-id area-id] database [router] [link-state-id]
show ip ospf [process-id area-id] database [network] [link-state-id]
show ip ospf [process-id area-id] database [summary] [link-state-id]
show ip ospf [process-id area-id] database [asb-summary] [link-state-id]
show ip ospf [process-id] database [external] [link-state-id]
show ip ospf [process-id area-id] database [database-summary]
```

Command Mode

EXEC

Syntax Description

process-id (Optional) Internally used identification parameter. It is locally assigned and can be any positive integer number. The number used here is the number assigned administratively when enabling the OSPF routing process.

area-id (Optional) Area number associated with the OSPF address range defined in the **network** router configuration command used to define the particular area.

link-state-id (Optional) Identifies the portion of the Internet environment that is being described by the advertisement. The value entered depends on the advertisement's LS type. It must be entered in the form of an IP address.

When the link state advertisement is describing a network, the *link-state-id* can take one of two forms:

—The network's IP address (as in type 3 summary link advertisements and in autonomous system external link advertisements).

—A derived address obtained from the link state ID. (Note that masking a network links advertisement's link state ID with the network's subnet mask yields the network's IP address.)

When the link state advertisement is describing a router, the link state ID is always the described router's OSPF router ID.

When an autonomous system external advertisement (LS Type = 5) is describing a default route, its link state ID is set to Default Destination (0.0.0.0).

When entered with the optional keyword **router**, **network**, **summary**, **asb-summary**, **external**, or **database-summary**, different displays result. Examples and brief descriptions of each form follow.

Sample Display of Show IP OSPF Database with No Arguments or Keywords

The following is sample output from the **show ip ospf database** command when no arguments or keywords are used:

```
Router# show ip ospf database
OSPF Router with id(190.20.239.66) (Autonomous system 300)
```

```
Displaying Router Link States(Area 0.0.0.0)

Link ID      ADV Router      Age      Seq#      Checksum  Link count
155.187.21.6 155.187.21.6  1731     0x80002CFB  0x69BC    8
155.187.21.5 155.187.21.5  1112     0x800009D2  0xA2B8    5
155.187.1.2   155.187.1.2   1662     0x80000A98  0x4CB6    9
155.187.1.1   155.187.1.1   1115     0x800009B6  0x5F2C    1
155.187.1.5   155.187.1.5   1691     0x80002BC   0x2A1A    5
155.187.65.6  155.187.65.6  1395     0x80001947  0xEEE1    4
155.187.241.5 155.187.241.5 1161     0x8000007C  0x7C70    1
155.187.27.6  155.187.27.6  1723     0x80000548  0x8641    4
155.187.70.6  155.187.70.6  1485     0x80000B97  0xEB84    6

Displaying Net Link States(Area 0.0.0.0)

Link ID      ADV Router      Age      Seq#      Checksum
155.187.1.3  192.20.239.66 1245     0x800000EC  0x82E

Displaying Summary Net Link States(Area 0.0.0.0)

Link ID      ADV Router      Age      Seq#      Checksum
155.187.240.0 155.187.241.5 1152     0x80000077  0x7A05
155.187.241.0 155.187.241.5 1152     0x80000070  0xAEB7
155.187.244.0 155.187.241.5 1152     0x80000071  0x95CB
```

Table 19-24 describes significant fields shown in the display.

Table 19-24 Show IP OSPF Database Field Descriptions

Field	Description
Link ID	Router ID number.
ADV Router	Advertising router's router ID.
Age	Link state age.
Seq#	Link state sequence number (detects old or duplicate link state advertisements).
Checksum	Fletcher checksum of the complete contents of the link state advertisement.
Link count	Number of interfaces detected for router.

Sample Display Using Show IP OSPF Database ASB-Summary

The following is sample output from the **show ip ospf database asb-summary** command when no optional arguments are specified:

```
Router# show ip ospf database asb-summary

OSPF Router with id(190.20.239.66) (Autonomous system 300)

        Displaying Summary ASB Link States(Area 0.0.0.0)

LS age: 1463
Options: (No TOS-capability)
LS Type: Summary Links(AS Boundary Router)
Link State ID: 155.187.245.1 (AS Boundary Router address)
Advertising Router: 155.187.241.5
LS Seq Number: 80000072
Checksum: 0x3548
Length: 28
Network Mask: 0.0.0.0 TOS: 0 Metric: 1
```

Table 19-25 describes significant fields shown in the display.

Table 19-25 Show IP OSPF Database ASB-Summary Field Descriptions

Field	Description
Router ID	Router ID number.
Autonomous system	OSPF autonomous system number (OSPF process ID).
LS age	Link state age.
Options	Type of Service options (Type 0 only).
LS Type	Link state type.
Link State ID	Link state ID (autonomous system boundary router).
Advertising Router	Advertising router's router ID.
LS Seq Number	Link state sequence (detects old or duplicate link state advertisements).
Checksum	LS checksum (Fletcher checksum of the complete contents of the link state advertisement).
Length	Length in bytes of the link state advertisement.
Network Mask	Network mask implemented.
TOS	Type of Service.
Metric	Link state metric.

Sample Display Using Show IP OSPF Database External

The following is sample output from the **show ip ospf database external** command when no optional arguments are specified:

```
Router# show ip ospf database external

OSPF Router with id(190.20.239.66) (Autonomous system 300)

Displaying AS External Link States

LS age: 280
Options: (No TOS-capability)
LS Type: AS External Link
Link State ID: 143.105.0.0 (External Network Number)
Advertising Router: 155.187.70.6
LS Seq Number: 80000AFD
Checksum: 0xC3A
Length: 36
Network Mask: 255.255.0.0
Metric Type: 2 (Larger than any link state path)
TOS: 0
Metric: 1
Forward Address: 0.0.0.0
External Route Tag: 0
```

Table 19-26 describes significant fields shown in the display.

Table 19-26 Show IP OSPF Database External Field Descriptions

Field	Description
Router ID	Router ID number.
Autonomous system	OSPF autonomous system number (OSPF process ID).
LS age	Link state age.
Options	Type of Service options (Type 0 only).
LS Type	Link state type.
Link State ID	Link state ID (External Network Number).
Advertising Router	Advertising router's router ID.
LS Seq Number	Link state sequence number (detects old or duplicate link state advertisements).
Checksum	LS checksum (Fletcher checksum of the complete contents of the link state advertisement).
Length	Length in bytes of the link state advertisement.
Network Mask	Network mask implemented.
Metric Type	External Type.
TOS	Type of Service.
Metric	Link state metric.
Forward Address	Forwarding address. Data traffic for the advertised destination will be forwarded to this address. If the forwarding address is set to 0.0.0.0, data traffic will be forwarded instead to the advertisement's originator.
External Route Tag	External route tag, a 32-bit field attached to each external route. This is not used by the OSPF protocol itself.

Sample Display Using Show IP OSPF Database Network

The following is sample output from the **show ip ospf database network** command when no optional arguments are specified:

```
Router# show ip ospf database network
OSPF Router with id(190.20.239.66) (Autonomous system 300)

Displaying Net Link States(Area 0.0.0.0)

LS age: 1367
Options: (No TOS-capability)
LS Type: Network Links
Link State ID: 155.187.1.3 (address of Designated Router)
Advertising Router: 190.20.239.66
LS Seq Number: 800000E7
Checksum: 0x1229
Length: 52
Network Mask: 255.255.255.0
Attached Router: 190.20.239.66
Attached Router: 155.187.241.5
Attached Router: 155.187.1.1
Attached Router: 155.187.54.5
Attached Router: 155.187.1.5
```

Table 19-27 describes significant fields shown in the display.

Table 19-27 Show IP OSPF Database Network Field Descriptions

Field	Description
OSPF Router with id	Router ID number.
Autonomous system 300	OSPF autonomous system number (OSPF process ID).
LS age:	Link state age.
Options:	Type of Service options (Type 0 only).
LS Type:	Link state type.
Link State ID	Link state ID of designated router.
Advertising Router	Advertising router's router ID.
LS Seq Number	Link state sequence (detects old or duplicate link state advertisements).
Checksum	LS checksum (Fletcher checksum of the complete contents of the link state advertisement).
Network Mask	Network mask implemented.
AS Boundary Router	Definition of router type.
Attached Router	List of routers attached to the network, by IP address.

Sample Display Using Show IP OSPF Database Router

The following is sample output from the **show ip ospf database router** command when no optional arguments are specified:

```
Router# show ip ospf database router

OSPF Router with id(190.20.239.66) (Autonomous system 300)

          Displaying Router Link States(Area 0.0.0.0)

LS age: 1176
Options: (No TOS-capability)
LS Type: Router Links
Link State ID: 155.187.21.6
Advertising Router: 155.187.21.6
LS Seq Number: 80002CF6
Checksum: 0x73B7
Length: 120
AS Boundary Router
155  Number of Links: 8

Link connected to: another Router (point-to-point)
(link ID) Neighboring Router ID: 155.187.21.5
(Link Data) Router Interface address: 155.187.21.6
Number of TOS metrics: 0
TOS 0 Metrics: 2
```

Table 19-28 describes significant fields shown in the display.

Table 19-28 Show IP OSPF Database Router Field Descriptions

Field	Description
OSPF Router with id	Router ID number.
Autonomous system	OSPF autonomous system number (OSPF process ID).
LS age	Link state age.
Options	Type of Service options (Type 0 only).
LS Type	Link state type.
Link State ID	Link state ID.
Advertising Router	Advertising router's router ID.
LS Seq Number	Link state sequence (detects old or duplicate link state advertisements).
Checksum	LS checksum (Fletcher checksum of the complete contents of the link state advertisement).
Length	Length in bytes of the link state advertisement.
AS Boundary Router	Definition of router type.
Number of Links	Number of active links.
link ID	Link type.
Link Data	Router interface address.
TOS	Type of Service metric (Type 0 only).

Sample Display Using Show IP OSPF Database Summary

The following is sample output from **show ip ospf database summary** command when no optional arguments are specified:

```
Router# show ip ospf database summary

OSPF Router with id(190.20.239.66) (Autonomous system 300)

Displaying Summary Net Link States(Area 0.0.0.0)

LS age: 1401
Options: (No TOS-capability)
LS Type: Summary Links(Network)
Link State ID: 155.187.240.0 (summary Network Number)
Advertising Router: 155.187.241.5
LS Seq Number: 80000072
Checksum: 0x84FF
Length: 28
Network Mask: 255.255.255.0    TOS: 0  Metric: 1
```

Table 19-29 describes significant fields shown in the display.

Table 19-29 Show IP OSPF Database Summary Field Descriptions

Field	Description
OSPF Router with id	Router ID number.
Autonomous system	OSPF autonomous system number (OSPF process ID).
LS age	Link state age.
Options	Type of Service options (Type 0 only).
LS Type	Link state type.
Link State ID	Link state ID (summary network number).
Advertising Router	Advertising router's router ID.
LS Seq Number	Link state sequence (detects old or duplicate link state advertisements).
Checksum	LS checksum (Fletcher checksum of the complete contents of the link state advertisement).
Length	Length in bytes of the link state advertisement.
Network Mask	Network mask implemented.
TOS	Type of Service.
Metric	Link state metric.

Sample Display Using Show IP OSPF Database Database-Summary

The following is sample output from **show ip ospf database database-summary** command when no optional arguments are specified:

```
Router# show ip ospf database database-summary

OSPF Router with ID (172.19.65.21) (Process ID 1)

  Area ID      Router      Network      Sum-Net      Sum-ASBR      Subtotal      Delete      Maxage
  202          1           0           0           0           1           0           0           0
  AS External
  Total        1           0           0           0           1           0           0           0
```

Table 19-30 describes significant fields shown in the display.

Table 19-30 Show IP OSPF Database Database-Summary Field Descriptions

Field	Description
Area ID	Area number.
Router	Number of router link state advertisements in that area.
Network	Number of network link state advertisements in that area.
Sum-Net	Number of summary link state advertisements in that area.
Sum-ASBR	Number of summary autonomous system boundary router (ASBR) link state advertisements in that area.
Subtotal	Sum of Router, Network, Sum-Net, and Sum-ASBR for that area.
Delete	Number of link state advertisements that are marked “Deleted” in that area.
Maxage	Number of link state advertisements that are marked “Maxaged” in that area.
AS External	Number of external link state advertisements.

show ip ospf interface

To display OSPF-related interface information, use the **show ip ospf interface** EXEC command.

show ip ospf interface [*type number*]

Syntax Description

<i>type</i>	(Optional) Interface type.
<i>number</i>	(Optional) Interface number.

Command Mode

EXEC

Sample Display

The following is sample output from the **show ip ospf interface** command when Ethernet 0 is specified:

```
Router# show ip ospf interface ethernet 0

Ethernet 0 is up, line protocol is up
  Internet Address 131.119.254.202, Mask 255.255.255.0, Area 0.0.0.0
  AS 201, Router ID 192.77.99.1, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State OTHER, Priority 1
  Designated Router id 131.119.254.10, Interface address 131.119.254.10
  Backup Designated router id 131.119.254.28, Interface addr 131.119.254.28
  Timer intervals configured, Hello 10, Dead 60, Wait 40, Retransmit 5
  Hello due in 0:00:05
  Neighbor Count is 8, Adjacent neighbor count is 2
    Adjacent with neighbor 131.119.254.28 (Backup Designated Router)
    Adjacent with neighbor 131.119.254.10 (Designated Router)
```

Table 19-31 describes significant fields shown in the display.

Table 19-31 Show IP OSPF Interface Ethernet 0 Field Descriptions

Field	Description
Ethernet	Status of physical link and operational status of protocol.
Internet Address	Interface IP address, subnet mask, and area address.
AS	Autonomous system number (OSPF process ID), router ID, network type, link state cost.
Transmit Delay	Transmit delay, interface state, and router priority.
Designated Router	Designated router ID and respective interface IP address.
Backup Designated router	Backup designated router ID and respective interface IP address.
Timer intervals configured	Configuration of timer intervals.
Hello	Number of seconds until next Hello packet is sent out this interface.
Neighbor Count	Count of network neighbors and list of adjacent neighbors.

show ip ospf neighbor

To display OSPF-neighbor information on a per-interface basis, use the **show ip ospf neighbor** EXEC command.

show ip ospf neighbor [type number] [neighbor-id] detail

Syntax Description

<i>type</i>	(Optional) Interface type.
<i>number</i>	(Optional) Interface number.
<i>neighbor-id</i>	(Optional) Neighbor ID.
detail	Displays all neighbors given in detail (list all neighbors).

Command Mode

EXEC

Sample Displays

The following is sample output from the **show ip ospf neighbor** command showing a single line of summary information for each neighbor:

```
Router# show ip ospf neighbor

      ID      Pri  State      Dead Time      Address      Interface
199.199.199.137 1    FULL/DR      0:00:31    160.89.80.37  Ethernet0
192.31.48.1     1    FULL/DROTHER  0:00:33    192.31.48.1   Fddi0
192.31.48.200   1    FULL/DROTHER  0:00:33    192.31.48.200 Fddi0
199.199.199.137 5    FULL/DR      0:00:33    192.31.48.189 Fddi0
```

The following is sample output showing summary information about the neighbor that matches the neighbor ID:

```
Router# show ip ospf neighbor 199.199.199.137

Neighbor 199.199.199.137, interface address 160.89.80.37
  In the area 0.0.0.0 via interface Ethernet0
  Neighbor priority is 1, State is FULL
  Options 2
  Dead timer due in 0:00:32
  Link State retransmission due in 0:00:04
Neighbor 199.199.199.137, interface address 192.31.48.189
  In the area 0.0.0.0 via interface Fddi0
  Neighbor priority is 5, State is FULL
  Options 2
  Dead timer due in 0:00:32
  Link State retransmission due in 0:00:03
```

If you specify the interface along with the Neighbor ID, the router displays the neighbors that match the neighbor ID on the interface, as in the following sample display:

```
Router# show ip ospf neighbor e 0 199.199.199.137

Neighbor 199.199.199.137, interface address 160.89.80.37
  In the area 0.0.0.0 via interface Ethernet0
  Neighbor priority is 1, State is FULL
```

show ip ospf neighbor

```
Options 2
Dead timer due in 0:00:37
Link State retransmission due in 0:00:04
```

You can also specify the interface without the neighbor ID to show all neighbors on the specified interface, as in the following sample display:

```
Router# show ip ospf neighbor f 0

      ID      Pri      State      Dead Time      Address      Interface
192.31.48.1      1      FULL/DROTHER  0:00:33      192.31.48.1      Fddi0
192.31.48.200    1      FULL/DROTHER  0:00:32      192.31.48.200    Fddi0
199.199.199.137  5      FULL/DR       0:00:32      192.31.48.189    Fddi0
```

The following is sample output from the **show ip ospf neighbor detail** command:

```
Router# show ip ospf neighbor detail

Neighbor 160.89.96.54, interface address 160.89.96.54
  In the area 0.0.0.3 via interface Ethernet0
  Neighbor priority is 1, State is FULL
  Options 2
  Dead timer due in 0:00:38
Neighbor 160.89.103.52, interface address 160.89.103.52
  In the area 0.0.0.0 via interface Serial0
  Neighbor priority is 1, State is FULL
  Options 2
  Dead timer due in 0:00:31
```

Table 19-32 describes the fields shown in the displays.

Table 19-32 Show IP OSPF Neighbor Field Descriptions

Field	Description
Neighbor x.x.x.x	Neighbor router ID.
interface address x.x.x.x	IP address of the interface.
In the area	Area and interface through which OSPF neighbor is known.
Neighbor priority	Router priority of neighbor, neighbor state.
State	OSPF state.
Options	Hello packet options field contents (E-bit only; possible values are 0 and 2; 2 indicates area is not a stub; 0 indicates area is a stub).
Dead timer	Expected time before router will declare neighbor dead.

show ip ospf virtual-links

To display parameters about and the current state of OSPF virtual links, use the **show ip ospf virtual-links** EXEC command.

show ip ospf virtual-links

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

Usage Guidelines

The information displayed by **show ip ospf virtual-links** is useful in debugging OSPF routing operations.

Sample Display

The following is sample output from the **show ip ospf virtual-links** command:

```
Router# show ip ospf virtual-links
Virtual Link to router 160.89.101.2 is up
Transit area 0.0.0.1, via interface Ethernet0, Cost of using 10
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 0:00:08
Adjacency State FULL
```

Table 19-33 describes significant fields shown in the display.

Table 19-33 Show IP OSPF Virtual-links Field Descriptions

Field	Description
Virtual Link to router 160.89.101.2	Specifies the OSPF neighbor, and if the link to that neighbor is Up or is Up.
Transit area 0.0.0.1	The transit area through which the virtual link is formed.
via interface Ethernet0	The interface through which the virtual link is formed.
Cost of using 10	The cost of reaching the OSPF neighbor through the virtual link.
Transmit Delay is 1 sec	The transmit delay on the virtual link.
State POINT_TO_POINT	The state of the OSPF neighbor.
Timer intervals...	The various timer intervals configured for the link.
Hello due in 0:00:08	When the next Hello is expected from the neighbor.
Adjacency State FULL	The adjacency state between the neighbors.

show ip pim interface

To display information about interfaces configured for PIM, use the **show ip pim interface** EXEC command.

show ip pim interface [*type number*]

Syntax Description

type (Optional) Interface type.
number (Optional) Interface number.

Command Mode

EXEC

Usage Guidelines

This command works only on interfaces that are configured for PIM.

Sample Display

The following is sample output from the **show ip pim interface** command:

```
Router# show ip pim interface
      Address          Interface        Mode    Neighbor  Query      DR
                           Count        Interval
 198.92.37.6      Ethernet0      Dense      2          30      198.92.37.33
 198.92.36.129    Ethernet1      Dense      2          30      198.92.36.131
 10.1.37.2        Tunnel0       Dense      1          30      0.0.0.0
```

Table 19-34 describes the fields shown in the display.

Table 19-34 Show IP PIM Interface Field Description

Field	Description
Address	IP address of the next-hop router.
Interface	Interface type and number that is configured to run PIM.
Mode	Multicast mode in which the router is operating. This can be dense mode or sparse mode. DVMRP indicates a DVMRP tunnel is configured.
Neighbor Count	Number of PIM neighbors that have been discovered through this interface. If the Neighbor Count is 1 for a DVMRP tunnel, the neighbor is active (receiving probes and reports).
Query Interval	Frequency, in seconds, of PIM router-query messages, as set by the ip pim query-interval interface configuration command. The default is 30 seconds.
DR	IP address of the designated router on the LAN. Note that serial lines do not have designated routers, so the IP address is shown as 0.0.0.0.

Related Commands

ip pim

show ip pim neighbor

show ip pim neighbor

To list the PIM neighbors discovered by the router, use the **show ip pim neighbor** EXEC command.

show ip pim neighbor [*type number*]

Syntax Description

<i>type</i>	(Optional) Interface type.
<i>number</i>	(Optional) Interface number.

Command Mode

EXEC

Usage Guidelines

Use this command to determine which routers on the LAN are configured for PIM.

Sample Display

The following is sample output from the **show ip pim neighbor** command:

```
Router# show ip pim neighbor

PIM Neighbor Table
Neighbor Address  Interface          Uptime      Expires    Mode
198.92.37.2       Ethernet0          17:38:16   0:01:25   Dense
198.92.37.33      Ethernet0          17:33:20   0:01:05   Dense (DR)
198.92.36.131     Ethernet1          17:33:20   0:01:08   Dense (DR)
198.92.36.130     Ethernet1          18:56:06   0:01:04   Dense
10.1.22.9         Tunnel0            19:14:59   0:01:09   Dense
```

Table 19-35 describes the fields shown in the display.

Table 19-35 Show IP PIM Neighbor Field Description

Field	Description
Neighbor Address	IP address of the PIM neighbor.
Interface	Interface type and number on which the neighbor is reachable.
Uptime	How long in hours, minutes, and seconds the entry has been in the PIM neighbor table.
Expires	How long in hours, minutes, and seconds until the entry will be removed from the IP multicast routing table.
Mode	Mode in which the interface is operating.
(DR)	Indicates that this neighbor is a designated router on the LAN.

Related Command

show ip pim interface

show ip pim rp

To display the rendezvous point (RP) routers associated with a sparse-mode multicast group, use the **show ip pim rp** EXEC command.

show ip pim rp [group-name | group-address]

Syntax Description

<i>group-name</i>	(Optional) Name of the multicast group, as defined in the DNS hosts table.
<i>group-address</i>	(Optional) Address of the multicast group. This is a multicast IP address in four-part dotted notation.

Command Mode

EXEC

Sample Displays

The following is sample output from the **show ip pim rp** command from a router that is not an RP:

```
Router1# show ip pim rp
Group: 224.2.127.255, number of RPs: 1
  RP address: 198.92.37.2, state: Up, uptime 0:01:25, expires in 0:03:04
```

The following is sample output from the **show ip pim rp** command from a router that is an RP:

```
Router2# show ip pim rp
Group: 224.2.127.255, number of RPs: 1
  RP address: 198.92.37.2, state: Up, next RP-reachable in 0:01:01
```

Table 19-36 explains the fields shown in the displays.

Table 19-36 Show IP PIM RP Field Description

Field	Description
Group:	Address of the multicast group.
number of RPs:	Number of RPs in the multicast group.
RP address:	Address of the RP.
state:	State of the RP router. It can be Up or Down.
uptime	How long in hours, minutes, and seconds the RP has been up.
expires	How long in hours, minutes, and seconds until the entry for this RP expires.
next RP-reachable in	How long in hours, minutes, and seconds until the RP will send its next RP-reachable message.

Related Command

show ip mroute

show ip protocols

To display the parameters and current state of the active routing protocol process, use the **show ip protocols** EXEC command.

show ip protocols

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

Usage Guidelines

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

Sample Displays

The following is sample output from the **show ip protocols** command, showing IGRP processes:

```
Router# show ip protocols

Routing Protocol is "igrp 109"
  Sending updates every 90 seconds, next due in 44 seconds
  Invalid after 270 seconds, hold down 280, flushed after 630
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  IGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  IGRP maximum hopcount 100
  IGRP maximum metric variance 1
  Redistributing: igrp 109
  Routing for Networks:
    198.92.72.0
  Routing Information Sources:
    Gateway          Distance      Last Update
    198.92.72.18      100          0:56:41
    198.92.72.19      100          6d19
    198.92.72.22      100          0:55:41
    198.92.72.20      100          0:01:04
    198.92.72.30      100          0:01:29
  Distance: (default is 100)

Routing Protocol is "bgp 1878"
  Sending updates every 60 seconds, next due in 0 seconds
  Outgoing update filter list for all interfaces is 1
  Incoming update filter list for all interfaces is not set
  Redistributing: igrp 109
  IGP synchronization is disabled
  Automatic route summarization is enabled
  Neighbor(s):
    Address          FiltIn FiltOut DistIn DistOut Weight RouteMap
    192.108.211.17          1
    192.108.213.89          1
```

```

198.6.255.13          1
198.92.72.18          1
198.92.72.19
198.92.84.17          1
Routing for Networks:
 192.108.209.0
 192.108.211.0
 198.6.254.0
Routing Information Sources:
  Gateway      Distance      Last Update
  198.92.72.19      20          0:05:28
Distance: external 20 internal 200 local 200

```

Table 19-37 describes significant fields shown in the display.

Table 19-37 Show IP Protocols Field Descriptions

Field	Description
Routing Protocol is “igrp 109”	Specifies the routing protocol used.
Sending updates every 90 seconds	Specifies the time between sending updates.
next due in 88 seconds	Precisely when the next update is due to be sent.
Invalid after 270 seconds	Specifies the value of the invalid parameter.
hold down for 280	Specifies the current value of the hold-down parameter.
flushed after 630	Specifies the time in seconds after which the individual routing information will be thrown (flushed) out.
Outgoing update ...	Specifies whether the outgoing filtering list has been set.
Incoming update ...	Specifies whether the incoming filtering list has been set.
Default networks	Specifies how these networks will be handled in both incoming and outgoing updates.
IGRP metric	Specifies the value of the K0-K5 metrics as well as the maximum hopcount.
Redistributing	Lists the protocol that is being redistributed.
Routing	Specifies the networks that the routing process is currently injecting routes for.
Routing Information Sources	Lists all the routing sources the router is using to build its routing table. For each source, you will see displayed: <ul style="list-style-type: none"> IP address Administrative distance Time the last update was received from this source.

The following is sample output from the **show ip protocols** command, showing Enhanced IGRP processes:

```

Router# show ip protocols

Routing Protocol is "eigrp 77"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Redistributing: eigrp 77
  Automatic network summarization is in effect
  Routing for Networks:
    160.89.0.0

```

```

Routing Information Sources:
  Gateway          Distance      Last Update
  160.89.81.28      90          0:02:36
  160.89.80.28      90          0:03:04
  160.89.80.31      90          0:03:04
  Distance: internal 90 external 170

```

Table 19-38 describes the fields that might be shown in the display.

Table 19-38 Show IP Protocols Field Descriptions

Field	Description
Routing Protocol is “eigrp 77”	Name and autonomous system number of the currently running routing protocol.
Outgoing update filter list for all interfaces...	Indicates whether a filter for outgoing routing updates has been specified with the distribute-list out command.
Outgoing update filter list for all interfaces...	Indicates whether a filter for outgoing routing updates has been specified with the distribute-list in command.
Redistributing: eigrp 77	Indicates whether route redistribution has been enabled with the redistribute command.
Automatic network summarization...	Indicates whether route summarization has been enabled with the auto-summary command.
Routing for Networks:	Networks that the routing process is currently injecting routes for.
Routing Information Sources:	Lists all the routing sources that the router is using to build its routing table. The following is displayed for each source: IP address, administrative distance, and time the last update was received from this source.
Distance: internal 90 external 170	Internal and external distances of the router. Internal distance is the degree of preference given to Enhanced IGRP internal routes. External distance is the degree of preference given to Enhanced IGRP external routes.

The following is sample output from the **show ip protocols** command, showing IS-IS processes:

```

Router# show ip protocols

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

```

show ip route

Use the **show ip route** EXEC command to display the current state of the routing table.

show ip route [address [mask] [longer-prefixes**]] | [protocol [process-id]]**

Syntax Description

<i>address</i>	(Optional) Address about which routing information should be displayed.
<i>mask</i>	(Optional) Argument for a subnet mask.
longer-prefixes	(Optional) The <i>address</i> and <i>mask</i> pair becomes a prefix and any routes that match that prefix are displayed.
<i>protocol</i>	(Optional) Name of a routing protocol; or the keyword connected , static , or summary . If you specify a routing protocol, use one of the following keywords: bgp , egp , eigrp , hello , igrp , isis , ospf , or rip .
<i>process-id</i>	(Optional) Number used to identify a process of the specified protocol.

Command Mode

EXEC

Sample Displays

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

```
Router# show ip route

Codes: I - IGRP derived, R - RIP derived, O - OSPF derived
      C - connected, S - static, E - EGP derived, B - BGP derived
      * - candidate default route, IA - OSPF inter area route
      E1 - OSPF external type 1 route, E2 - OSPF external type 2 route

Gateway of last resort is 131.119.254.240 to network 129.140.0.0

O E2 150.150.0.0 [160/5] via 131.119.254.6, 0:01:00, Ethernet2
E   192.67.131.0 [200/128] via 131.119.254.244, 0:02:22, Ethernet2
O E2 192.68.132.0 [160/5] via 131.119.254.6, 0:00:59, Ethernet2
O E2 130.130.0.0 [160/5] via 131.119.254.6, 0:00:59, Ethernet2
E   128.128.0.0 [200/128] via 131.119.254.244, 0:02:22, Ethernet2
E   129.129.0.0 [200/129] via 131.119.254.240, 0:02:22, Ethernet2
E   192.65.129.0 [200/128] via 131.119.254.244, 0:02:22, Ethernet2
E   131.131.0.0 [200/128] via 131.119.254.244, 0:02:22, Ethernet2
E   192.75.139.0 [200/129] via 131.119.254.240, 0:02:23, Ethernet2
E   192.16.208.0 [200/128] via 131.119.254.244, 0:02:22, Ethernet2
E   192.84.148.0 [200/129] via 131.119.254.240, 0:02:23, Ethernet2
E   192.31.223.0 [200/128] via 131.119.254.244, 0:02:22, Ethernet2
E   192.44.236.0 [200/129] via 131.119.254.240, 0:02:23, Ethernet2
E   140.141.0.0 [200/129] via 131.119.254.240, 0:02:22, Ethernet2
E   141.140.0.0 [200/129] via 131.119.254.240, 0:02:23, Ethernet2
```

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

```
Router# show ip route

Codes: I - IGRP derived, R - RIP derived, O - OSPF derived
      C - connected, S - static, E - EGP derived, B - BGP derived
      i - IS-IS derived
      * - candidate default route, IA - OSPF inter area route
      E1 - OSPF external type 1 route, E2 - OSPF external type 2 route
      L1 - IS-IS level-1 route, L2 - IS-IS level-2 route

Gateway of last resort is not set

      160.89.0.0 is subnetted (mask is 255.255.255.0), 3 subnets
C          160.89.64.0 255.255.255.0 is possibly down,
           routing via 0.0.0.0, Ethernet0
i L2      160.89.67.0 [115/20] via 160.89.64.240, 0:00:12, Ethernet0
i L2      160.89.66.0 [115/20] via 160.89.64.240, 0:00:12, Ethernet0
```

Table 19-39 describes significant fields shown in these two displays.

Table 19-39 Show IP Route Field Descriptions

Field	Description
O	Indicates protocol that derived the route. Possible values include: <ul style="list-style-type: none"> I—IGRP derived R—RIP derived O—OSPF derived C—connected S—static E—EGP derived B—BGP derived i—IS-IS derived
E2	Type of route. Possible values include: <ul style="list-style-type: none"> *—Indicates the last path used when a packet was forwarded. It pertains only to the nonfast-switched packets. However, it does not indicate what path will be used next when forwarding a nonfast-switched packet except when the paths are equal cost. IA—OSPF interarea route E1—OSPF external type 1 route E2—OSPF external type 2 route L1—IS-IS Level 1 route L2—IS-IS Level 2 route
150.150.0.0	Indicates the address of the remote network.
[160/5]	The first number in the brackets is the administrative distance of the information source; the second number is the metric for the route.
via 131.119.254.6	Specifies the address of the next router to the remote network.
0:01:00	Specifies the last time the route was updated in hours:minutes:seconds.
Ethernet 2	Specifies the interface through which the specified network can be reached.

When you specify that you want information about a specific network displayed, more detailed statistics are shown. The following is sample output from the **show ip route** command when entered with the address 131.119.0.0.

```
Router# show ip route 131.119.0.0

Routing entry for 131.119.0.0 (mask 255.255.0.0)
  Known via "igrp 109", distance 100, metric 10989
    Tag 0
    Redistributing via igrp 109
    Last update from 131.108.35.13 on TokenRing0, 0:00:58 ago
    Routing Descriptor Blocks:
      * 131.108.35.13, from 131.108.35.13, 0:00:58 ago, via TokenRing0
        Route metric is 10989, traffic share count is 1
        Total delay is 45130 microseconds, minimum bandwidth is 1544 Kbit
        Reliability 255/255, minimum MTU 1500 bytes
        Loading 2/255, Hops 4
```

Table 19-40 describes significant fields shown in the display.

Table 19-40 Show IP Route with Address Field Descriptions

Field	Description
Routing entry for 131.119.0.0 (mask 255.255.0.0)	Network number and mask.
Known via "igrp 109"	Indicates how the route was derived.
distance 100	Administrative distance of the information source.
Tag 0	Integer that is used to implement the route.
Redistributing via igrp 109	Indicates redistribution protocol.
Last update from 131.108.35.13 on TokenRing0	Indicates the IP address of a router that is the next hop to the remote network and the router interface on which the last update arrived.
0:00:58 ago	Specifies the last time the route was updated in hours:minutes:seconds.
131.108.35.13, from 131.108.35.13, 0:00:58 ago	Indicates the next hop address, the address of the gateway that sent the update, and the time that has elapsed since this update was received in hours:minutes:seconds.
via TokenRing0	Interface for this route.
Route metric is 10989	This value is the best metric for this routing descriptor block.
traffic share count is 1	Number of uses for this routing descriptor block.
Total delay is 45130 microseconds	Total propagation delay in microseconds.
minimum bandwidth is 1544 Kbit	Minimum bandwidth encountered when transmitting data along this route.
Reliability 255/255	Likelihood of successful packet transmission expressed as a number between 0 and 255 (255 is 100% reliability).
minimum MTU 1500 bytes	Smallest MTU along the path.
Loading 2/255	Effective bandwidth of the route in kilobits per second/255 is saturation.
Hops 4	Hops to the destination or to the router where the route first enters IGRP.

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

In the following example, the logical AND operation is performed on the source address 128.0.0.0 and the mask 128.0.0.0, resulting in 128.0.0.0. Each destination in the routing table is also logically ANDed with the mask and compared to that result of 128.0.0.0. Any destinations that fall into that range are displayed in the output.

```
Router# show ip route 128.0.0.0 128.0.0.0 longer-prefixes

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default

Gateway of last resort is not set

S      134.134.0.0 is directly connected, Ethernet0
S      131.131.0.0 is directly connected, Ethernet0
S      129.129.0.0 is directly connected, Ethernet0
S      128.128.0.0 is directly connected, Ethernet0
S      198.49.246.0 is directly connected, Ethernet0
S      192.160.97.0 is directly connected, Ethernet0
S      192.153.88.0 is directly connected, Ethernet0
S      192.76.141.0 is directly connected, Ethernet0
S      192.75.138.0 is directly connected, Ethernet0
S      192.44.237.0 is directly connected, Ethernet0
S      192.31.222.0 is directly connected, Ethernet0
S      192.16.209.0 is directly connected, Ethernet0
S      144.145.0.0 is directly connected, Ethernet0
S      140.141.0.0 is directly connected, Ethernet0
S      139.138.0.0 is directly connected, Ethernet0
S      129.128.0.0 is directly connected, Ethernet0
      172.19.0.0 255.255.255.0 is subnetted, 1 subnets
C          172.19.64.0 is directly connected, Ethernet0
      171.69.0.0 is variably subnetted, 2 subnets, 2 masks
C          171.69.232.32 255.255.255.240 is directly connected, Ethernet0
S          171.69.0.0 255.255.0.0 is directly connected, Ethernet0
Router#
```

Related Commands

A dagger (†) indicates that the command is documented in another chapter.

show interfaces tunnel †
show ip route summary

show ip route summary

To display the current state of the routing table, use the **show ip route summary** EXEC command.

show ip route summary

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

Sample Display

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

```
Router# show ip route summary
  Route  Source      Networks   Subnets   Overhead   Memory (bytes)
connected      0          3          126        360
static         1          2          126        360
igrp 109      747        12         31878      91080
internal       3          0          0          360
Total          751        17         32130      92160
Router#
```

Table 19-41 describes the fields shown in the display:

Table 19-41 Show IP Route Summary Field Descriptions

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

Related Command

show ip route

show ip route supernets-only

To display information about supernets, use the **show ip route supernets-only** privileged EXEC command.

show ip route supernets-only

Command Mode

Privileged EXEC

Sample Display

The following is sample output from the **show ip route supernets-only** command:

```
Router# show ip route supernets-only

Codes: I - IGRP derived, R - RIP derived, O - OSPF derived
      C - connected, S - static, E - EGP derived, B - BGP derived
      i - IS-IS derived, D - EIGRP derived
      * - candidate default route, IA - OSPF inter area route
      E1 - OSPF external type 1 route, E2 - OSPF external type 2 route
      L1 - IS-IS level-1 route, L2 - IS-IS level-2 route
      EX - EIGRP external route

Gateway of last resort is not set

B    198.92.0.0 (mask is 255.255.0.0) [20/0] via 198.92.72.30, 0:00:50
B    192.0.0.0 (mask is 255.0.0.0) [20/0] via 198.92.72.24, 0:02:50
Router#
```

This display shows supernets only; it does not show subnets.

show ip sd

To display the contents of the session directory cache, use the **show ip sd** EXEC command.

show ip sd [group / “session-name” / detail]

Syntax Description

<i>group</i>	(Optional) Displays the session(s) defining the multicast group in detail format.
“ <i>session-name</i> ”	(Optional) Displays the single session in detail format. Can be in uppercase or lowercase and still match. The session name is enclosed in quotation marks.
detail	(Optional) Displays all sessions in detail format.

Command Mode

EXEC

Usage Guidelines

If the router is configured to be a member of 224.2.127.255 (the default session directory group), it will cache session directory announcements. If no arguments are used, a sorted list of session names is displayed.

Sample Display

The following is sample output from the **show ip sd** command, showing each session that the router has learned:

```
Router> show ip sd

SD Cache - 22 entries
  *cisco: CABONE Audio
  *cisco: CABONE Video
  *cisco: CABONE Whiteboard
  *cisco: CBONE audio
  *cisco: CBONE video
  *cisco: CBONE Whiteboard
  *cisco: CCIE Audio
  *cisco:Eng Services Ops Review
  *cisco:Scamp's Managers Meeting
  A3TEST
  aki
  APLtest
  arch-nus
  Bharat Dave-ETH
  cbone
  CERN - LHCC
  cisco: Beta Folks
  DB
  DECUS '95: Marc Andreessen (audio)
  DECUS '95: Marc Andreessen (vic/h261)
  Digital Unix Multicast
  DSTC Fun with whiteboard
```

The following is sample output from the **show ip sd detail** command:

```
Router# show ip sd detail

SD Cache - 3 entries
Session Name: *cisco: CABONE Audio
  Description: cisco Customer Advocacy Audio Channel
  Group: 224.0.255.128, ttl: 16
  Lifetime: from 00:00:24 PDT May 9 1995 until 00:00:24 PDT May 23 1995
  Created by: bpinsky@on-tap.cisco.com (171.68.225.179)
  Media: audio 55557 2688
--More--
Session Name: *cisco: CABONE Video
  Description: cisco Customer Advocacy Video Channel
  Group: 224.0.255.130, ttl: 16
  Lifetime: from 00:00:56 PDT May 9 1995 until 00:00:56 PDT May 23 1995
  Created by: bpinsky@on-tap.cisco.com (171.68.225.179)
  Media: video 62676 63933
--More--
Session Name: *cisco: CABONE Whiteboard
  Description: cisco Customer Advocacy Whiteboard
  Group: 224.0.255.129, ttl: 16
  Lifetime: from 00:00:30 PDT May 9 1995 until 00:00:30 PDT May 23 1995
  Created by: bpinsky@on-tap.cisco.com (171.68.225.179)
  Media: whiteboard 43411 14736
```

Table 19-42 describes the significant fields in the display.

Table 19-42 Show IP SD Field Descriptions

Field	Description
Session Name	Name of the session.
Description	Description of the session.
Group	Group address.
ttl	Time-to-live for the session.
Lifetime	Lifetime of the session advertisement.
Created by	Creator of the session.
Media	Type of media, port number and conference ID.

show isis database

To display the IS-IS link state database, use the **show isis database** EXEC command.

show isis database [level-1] [level-2] [l1] [l2] [detail] [lspid]

Syntax Description

level-1	(Optional) Displays the IS-IS link state database for Level 1.
level-2	(Optional) Displays the IS-IS link state database for Level 2.
l1	(Optional) Abbreviation for the option level-1 .
l2	(Optional) Abbreviation for the option level-2 .
detail	(Optional) When specified, the contents of each LSP is displayed. Otherwise, a summary display is provided.
lspid	(Optional) Link-state protocol ID. When specified, the contents of a single LSP is displayed by its ID number.

Command Mode

EXEC

Usage Guidelines

Each of the options shown in brackets for this command can be entered in an arbitrary string within the same command entry. For example, the following are both valid command specifications and provide the same output: **show isis database detail l2** and **show isis database l2 detail**.

Sample Display

The following is sample output from the **show isis database** command when it is specified with no options or as **show isis database l1 l2**:

```
Router# show isis database

IS-IS Level-1 Link State Database
LSPID          LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
0000.0C00.0C35.00-00 0x0000000C 0x5696        792          0/0/0
0000.0C00.40AF.00-00* 0x00000009 0x8452        1077         1/0/0
0000.0C00.62E6.00-00 0x0000000A 0x38E7        383          0/0/0
0000.0C00.62E6.03-00 0x00000006 0x82BC        384          0/0/0
0800.2B16.24EA.00-00 0x00001D9F 0x8864        1188         1/0/0
0800.2B16.24EA.01-00 0x00001E36 0x0935        1198         1/0/0

IS-IS Level-2 Link State Database
LSPID          LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
0000.0C00.0C35.03-00 0x00000005 0x04C8        792          0/0/0
0000.0C00.3E51.00-00 0x00000007 0xAF96        758          0/0/0
0000.0C00.40AF.00-00* 0x0000000A 0x3AA9        1077         0/0/0
```

Table 19-43 describes significant fields shown in the display.

Table 19-43 Show IS-IS Database Field Descriptions

Field	Description
LSPID	The link state PDU ID. The first six octets form the System ID. The next octet is the pseudo ID. When this value is zero, the LSP describes links from the system. When it is nonzero, the LSP is a pseudonode LSP. The designated router for an interface is the only system that originates pseudonode LSPs. The last octet is the LSP number. If there is more data than can fit in a single LSP, additional LSPs are sent with increasing LSP numbers. An asterisk (*) indicates that the LSP was originated by the local system.
LSP Seq Num	Sequence number for the LSP that allows other systems to determine if they have received the latest information from the source.
LSP Checksum	Checksum of the entire LSP packet.
LSP Holdtime	Amount of time the LSP remains valid, in seconds.
ATT	The attach bit. This indicates that the router is also a Level 2 router, and it can reach other areas.
P	The P bit. Detects if the IS is area partition repair capable.
OL	The Overload bit. Determines if the IS is congested.

Sample Display Using Show IS-IS Database Detail

The following is sample output from the **show isis database detail** command.

```
Router# show isis database detail

IS-IS Level-1 Link State Database
LSPID          LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
0000.0C00.0C35.00-00 0x0000000C  0x5696        325          0/0/0
  Area Address: 47.0004.004D.0001
  Area Address: 39.0001
  Metric: 10   IS 0000.0C00.62E6.03
  Metric: 0    ES 0000.0C00.0C35
  --More--
0000.0C00.40AF.00-00* 0x00000009  0x8452        608          1/0/0
  Area Address: 47.0004.004D.0001
  Metric: 10   IS 0800.2B16.24EA.01
  Metric: 10   IS 0000.0C00.62E6.03
  Metric: 0    ES 0000.0C00.40AF

IS-IS Level-2 Link State Database
LSPID          LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
0000.0C00.0C35.03-00 0x00000005  0x04C8        317          0/0/0
  Metric: 0    IS 0000.0C00.0C35.00
  --More--
0000.0C00.3E51.00-00 0x00000009  0xAB98        1182         0/0/0
  Area Address: 39.0004
  Metric: 10   IS 0000.0C00.40AF.00
  Metric: 10   IS 0000.0C00.3E51.05
```

As the output shows, in addition to the information displayed with **show isis database**, the **show isis database detail** command displays the contents of each LSP.

Table 19-44 describes the fields shown in the display.

Table 19-44 Show IS-IS Database Detail Field Descriptions

Field	Description
LSPID	The link state PDU ID. The first six octets form the System ID. The next octet is the pseudo ID. When this value is zero, the LSP describes links from the system. When it is nonzero, the LSP is a pseudonode LSP. The designated router for an interface is the only system that originates pseudonode LSPs. The last octet is the LSP number. If there is more data than can fit in a single LSP, additional LSPs are sent with increasing LSP numbers. An asterisk (*) indicates that the LSP was originated by the local system.
LSP Seq Num	Sequence number for the LSP that allows other systems to determine if they have received the latest information from the source.
LSP Checksum	Checksum of the entire LSP packet.
LSP Holdtime	Amount of time the LSP remains valid, in seconds.
ATT	The attach bit. This indicates that the router is also a Level 2 router, and it can reach other areas.
P	The P bit. Detects if the IS is area partition repair capable.
OL	The Overload bit. Determines if the IS is congested.
Area Address:	Reachable area addresses from the router.
Metric:	IS-IS metric for the route.

Sample Display Using Show IS-IS Database Detail Displaying IP Addresses

The following is additional sample output from the **show isis database detail** command. This is a Level 2 LSP. The area address 39.0001 is the address of the area in which the router resides.

```
Router# show isis database detail 12

IS-IS Level-2 Link State Database
LSPID          LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
0000.0C00.1111.00-00* 0x00000006  0x4DB3        1194        0/0/0
  Area Address: 39.0001
  NLPID:        0x81 0xCC
  IP Address:  160.89.64.17
  Metric: 10   IS 0000.0C00.1111.09
  Metric: 10   IS 0000.0C00.1111.08
  Metric: 10   IP 160.89.65.0 255.255.255.0
  Metric: 10   IP 160.89.64.0 255.255.255.0
  Metric: 0    IP-External 10.0.0.0 255.0.0.0
```

Table 19-45 describes the fields shown in the display.

Table 19-45 Show IS-IS Database Detail Field Descriptions

Field	Description
LSPID	The link state PDU ID. The first six octets form the System ID. The next octet is the pseudo ID. When this value is zero, the LSP describes links from the system. When it is nonzero, the LSP is a pseudonode LSP. The designated router for an interface is the only system that originates pseudonode LSPs. The last octet is the LSP number. If there is more data than can fit in a single LSP, additional LSPs are sent with increasing LSP numbers. An asterisk (*) indicates that the LSP was originated by the local system.

show isis database

Field	Description
LSP Seq Num	Sequence number for the LSP that allows other systems to determine if they have received the latest information from the source.
LSP Checksum	Checksum of the entire LSP packet.
LSP Holdtime	Amount of time the LSP remains valid, in seconds.
ATT	The attach bit. This indicates that the router is also a Level 2 router, and it can reach other areas.
P	The P bit. Detects if the IS is area partition repair capable.
OL	The Overload bit. Determines if the IS is congested.
Area Address:	Reachable area addresses from the router.
NLPID	Indicates that both IP and OSI (0x0cc and 0x081 respectively) are supported in IS-IS for this router.
IP Address:	The IP address for the router is advertised in the LSP.
Metric:	IS-IS metric for the route.
Various addresses	The “IP” entries are the directly connected IP subnets the router is advertising (with associated metrics). The “IP-External” is a redistribute route.

show route-map

To display configured route-maps, use the **show route-map** EXEC command.

show route-map [map-name]

Syntax Description

map-name (Optional) Name of a specific route-map.

Command Mode

EXEC

Sample Display

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

```
Router# show route-map

route-map foo, permit, sequence 10
  Match clauses:
    tag 1 2
  Set clauses:
    metric 5
route-map foo, permit, sequence 20
  Match clauses:
    tag 3 4
  Set clauses:
    metric 6
```

Table 19-46 describes the fields shown in the display:

Table 19-46 Show Route-map Field Descriptions

Field	Description
route-map	Name of the route-map.
permit	Indicates that the route is redistributed as controlled by the set actions.
sequence	Number that indicates the position a new route map is to have in the list of route maps already configured with the same name.
Match clauses	Match criteria—conditions under which redistribution is allowed for the current route-map.
tag	
Set clauses	Set actions—the particular redistribution actions to perform if the criteria enforced by the match commands are met.
metric	

Related Commands

redistribute
route-map

summary-address

Use the **summary-address** router configuration command to create aggregate addresses for IS-IS or OSPF. The **no summary-address** command restores the default.

```
summary-address address mask {level-1 | level-1-2 | level-2}  
no summary-address address mask {level-1 | level-1-2 | level-2}
```

Syntax Description

<i>address</i>	Summary address designated for a range of addresses.
<i>mask</i>	IP subnet mask used for the summary route.
level-1	Only routes redistributed into Level 1 are summarized with the configured address/mask value. This keyword does not apply to OSPF.
level-1-2	The summary router is injected into both a Level 1 area and a Level 2 subdomain. This keyword does not apply to OSPF.
level-2	Routes learned by Level 1 routing will be summarized into the Level 2 backbone with the configured address/mask value. This keyword does not apply to OSPF.

Default

Disabled

Command Mode

Router configuration

Usage Guidelines

Multiple groups of addresses can be summarized for a given level. Routes learned from other routing protocols can also be summarized. The metric used to advertise the summary is the smallest metric of all the more specific routes. This command helps reduce the size of the routing table.

Using this command for OSPF causes an OSPF Autonomous System Boundary Router (ASBR) to advertise one external route as an aggregate for all redistributed routes that are covered by the address. For OSPF, this command summarizes only routes from other routing protocols that are being redistributed into OSPF. Use the **area range** command for route summarization between OSPF areas.

Example for IS-IS

In the following example, summary address 10.1.0.0 includes address 10.1.1, 10.1.2, 10.1.3, 10.1.4, and so forth. Only the address 10.1.0.0 is advertised in an IS-IS Level 1 Link State PDU.

```
summary-address 10.1.0.0 255.255.0.0 level-1
```

Example for OSPF

In the following example, summary address 10.1.0.0 includes address 10.1.1.0, 10.1.2.0, 10.1.3.0, and so forth. Only the address 10.1.0.0 is advertised in an external link state advertisement.

```
summary-address 10.1.0.0 255.255.0.0
```

Related Command**area range**

synchronization

To enable the synchronization between BGP and your IGP, use the **synchronization** router configuration command. To enable a router to advertise a network route without waiting for the IGP, use the **no** form of this command.

```
synchronization  
no synchronization
```

Syntax Description

This command has no arguments or keywords.

Default

Enabled

Command Mode

Router configuration

Usage Guidelines

Usually, a BGP speaker does not advertise a route to an external neighbor unless that route is local or exists in the IGP. The **no synchronization** command allows a router to advertise a network route without waiting for the IGP. This feature allows routers within an autonomous system to have the route before BGP makes it available to other autonomous systems.

Use **synchronization** if there are routers in the autonomous system that do not speak BGP.

Example

The following example enables the router to advertise a network route without waiting for the IGP:

```
router bgp 120  
no synchronization
```

table-map

To modify metric and tag values when the IP routing table is updated with BGP learned routes, use the **table-map** router configuration command. To disable this function, use the **no** form of the command.

table-map *route-map-name*
no table-map *route-map-name*

Syntax Description

route-map-name Route map name, from the **route-map** command.

Default

Disabled

Command Mode

Router configuration

Usage Guidelines

This command adds the route map name defined by the **route-map** command to the IP routing table. This command is used to set the tag name and the route metric to implement redistribution.

You can use **match** clauses of route maps in the **table-map** command. IP access list, autonomous system paths, and next-hop match clauses are supported.

Example

In the following example, the router is configured to automatically compute the tag value for the BGP learned routes and to update the IP routing table.

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

Related Commands

match as-path
match ip address
match ip next-hop
route-map

timers basic (EGP, RIP, IGRP)

To adjust EGP, RIP, or IGRP network timers, use the **timers basic** router configuration command. To restore the default timers, use the **no** form of this command.

timers basic *update invalid holddown flush [sleeptime]*
no timers basic

Syntax Description

<i>update</i>	Rate in seconds at which updates are sent. This is the fundamental timing parameter of the routing protocol.
<i>invalid</i>	Interval of time in seconds after which a route is declared invalid; it should be three times the value of <i>update</i> . A route becomes invalid when there is an absence of updates that refresh the route. The route then enters holddown. The route is marked inaccessible and advertised as unreachable. However, the route is still used for forwarding packets.
<i>holddown</i>	Interval in seconds during which routing information regarding better paths is suppressed. It should be at least three times the value of <i>update</i> . A route enters into a holddown state when an update packet is received that indicates the route is unreachable. The route is marked inaccessible and advertised as unreachable. However, the route is still used for forwarding packets. When holddown expires, routes advertised by other sources are accepted and the route is no longer inaccessible.
<i>flush</i>	Amount of time in seconds that must pass before the route is removed from the routing table; the interval specified must be at least the sum of <i>invalid</i> and <i>holddown</i> . If it is less than this sum, the proper holddown interval cannot elapse, which results in a new route being accepted before the holddown interval expires.
<i>sleeptime</i>	(Optional) For IGRP only, interval in milliseconds for postponing routing updates in the event of a flash update. The <i>sleeptime</i> value should be less than the <i>update</i> time. If the <i>sleeptime</i> is greater than the <i>update</i> time, routing tables will become unsynchronized.

Defaults

Protocol	<i>update</i>	<i>invalid</i>	<i>holddown</i>	<i>flush</i>	<i>sleeptime</i>
EGP	N/A	1080	N/A	1200	N/A
RIP	30	180	180	240	N/A
IGRP	90	270	280	630	0

Command Mode

Router configuration

Usage Guidelines

The basic timing parameters for IGRP, EGP, and RIP are adjustable. Since these routing protocols are executing a distributed, asynchronous routing algorithm, it is important that these timers be the same for all routers in the network.

Note The current and default timer values can be seen by inspecting the output of the **show ip protocols** EXEC command. The relationships of the various timers should be preserved as described previously.

Examples

In the following example, updates are broadcast every 5 seconds. If a router is not heard from in 15 seconds, the route is declared unusable. Further information is suppressed for an additional 15 seconds. At the end of the suppression period, the route is flushed from the routing table.

```
router igrp 109
timers basic 5 15 15 30
```

Note that by setting a short update period, you run the risk of congesting slow-speed serial lines; however, this is not a big concern on faster-speed Ethernets and T1-rate serial lines. Also, if you have many routes in your updates, you can cause the routers to spend an excessive amount of time processing updates.

When the **timers basic** command is used with EGP, the update time and holddown time are ignored. For example, the commands that follow will set the invalid time for EGP to 100 seconds and the flush time to 200 seconds.

```
router egp 47
timers basic 0 100 0 200
```

timers bgp

To adjust BGP network timers, use the **timers bgp** router configuration command. To reset the BGP timing defaults, use the **no** form of this command.

```
timers bgp keepalive holdtime  
no timers bgp
```

Syntax Description

<i>keepalive</i>	Frequency, in seconds, with which the router sends <i>keepalive</i> messages to its peer. The default is 60 seconds.
<i>holdtime</i>	Interval, in seconds, after not receiving a <i>keepalive</i> message that the router declares a peer dead. The default is 180 seconds.

Defaults

keepalive: 60 seconds
holdtime: 180 seconds

Command Mode

Router configuration

Example

The following example changes the *keepalive* timer to 70 seconds and the *holdtime* timer to 210 seconds:

```
timers bgp 70 210
```

Related Commands

clear ip bgp
router bgp
show ip bgp

timers egp

To adjust EGP Hello and polltime network timers, use the **timers egp** router configuration command. The **no** form of this command resets the EGP timing defaults.

```
timers egp hello polltime
no timers egp
```

Syntax Description

<i>hello</i>	Frequency, in seconds, with which the router sends Hello messages to its peer. The default is 60 seconds.
<i>polltime</i>	Interval, in seconds, for how frequently to exchange updates. The default is 180 seconds.

Defaults

hello: 60 seconds
polltime: 180 seconds

Command Mode

Router configuration

Usage Guidelines

To change the invalid time or flush time for EGP routes, use the **timers basic** router configuration command.

Example

The following example changes the EGP timers to 2 minutes and 5 minutes, respectively:

```
timers egp 120 300
```

Related Commands

router egp
show ip egp
timers basic (EGP, RIP, IGRP)

timers spf

To configure the delay time between when OSPF receives a topology change and when it starts a Shortest Path First (SPF) calculation, and the hold time between two consecutive SPF calculations, use the **timers spf** router configuration command. To return to the default timer values, use the **no** form of this command.

```
timers spf spf-delay spf-holddate  
no timers spf spf-delay spf-holddate
```

Syntax Description

<i>spf-delay</i>	Delay time, in seconds, between when OSPF receives a topology change and when it starts a SPF. calculation. It can be an integer from 0 to 65535. The default time is 5 seconds. A value of 0 means that there is no delay; that is, the SPF calculation is started immediately.
<i>spf-holddate</i>	Minimum time, in seconds, between two consecutive SPF calculations. It can be an integer from 0 to 65535. The default time is 10 seconds. A value of 0 means that there is no delay; that is, two consecutive SPF calculations can be done one immediately after the other.

Defaults

spf-delay: 5 seconds
spf-holddate: 10 seconds

Command Mode

Router configuration

Usage Guidelines

Setting the delay and hold time low causes routing to switch to the alternate path more quickly in the event of a failure. However, it consumes more CPU processing time.

Example

The following example changes the delay to 10 seconds and the hold time to 20 seconds:

```
timers spf 10 20
```

traffic-share

To control how traffic is distributed among routes when there are multiple routes for the same destination network that have different costs, use the **traffic-share** router configuration command. To disable this function, use the **no** form of the command.

```
traffic-share {balanced | min}  
[no] traffic share {balanced | min}
```

Syntax Description

balanced	Distributes traffic proportionately to the ratios of the metrics.
min	Uses routes that have minimum costs.

Default

Traffic is distributed proportionately to the ratios of the metrics.

Command Mode

Router configuration

Usage Guidelines

This command applies to IGRP and Enhanced IGRP routing protocols only. With the default setting, routes that have higher metrics represent less-preferable routes and get less traffic. Configuring **traffic-share min** causes the router to only divide traffic among the routes with the best metric. Other routes will remain in the routing table, but will receive no traffic.

Example

In the following example, only routes of minimum cost will be used:

```
router igrp 5  
traffic-share min
```

validate-update-source

To have the router to validate the source IP address of incoming routing updates for RIP and IGRP routing protocols, use the **validate-update-source** router configuration command. To disable this function, use the **no** form of this command.

```
validate-update-source  
no validate-update-source
```

Syntax Description

This command has no arguments or keywords.

Default

Enabled

Command Mode

Router configuration

Usage Guidelines

This command is only applicable to RIP and IGRP. The router ensures that the source IP address of incoming routing updates is on the same IP network as one of the addresses defined for the receiving interface.

Disabling split horizon on the incoming interface will also cause the system to perform this validation check.

For unnumbered IP interfaces (interfaces configured as **ip unnumbered**), no checking is performed.

Example

In the following example, the router is configured to not perform validation checks on the source IP address of incoming RIP updates:

```
router rip
network 128.105.0.0
no validate-update-source
```

variance

To control load balancing in an Enhanced IGRP-based internetwork, use the **variance** router configuration command. To reset the variance to the default value, use the **no** form of this command.

```
variance multiplier  
no variance
```

Syntax Description

<i>multiplier</i>	Metric value used for load balancing. It can be a value from 1 to 128. The default is 1, which means equal-cost load balancing.
-------------------	---

Default

1 (equal-cost load balancing)

Command Mode

Router configuration

Usage Guidelines

Setting a variance value lets the router determine the feasibility of a potential route. A route is feasible if the next router in the path is closer to the destination than the current router and if the metric for the entire path is within the variance. Only paths that are feasible can be used for load balancing and included in the routing table.

If the following two conditions are met, the route is deemed feasible and can be added to the routing table:

- 1 The local best metric must be greater than the metric learned from the next router.
- 2 The multiplier times the local best metric for the destination must be greater than or equal to the metric through the next router.

Example

The following example sets a variance value of 4:

```
router igrp 109  
variance 4
```

