



BGP Commands

Use the commands in this chapter to configure and monitor Border Gateway Protocol (BGP). For BGP configuration information and examples, refer to the “Configuring BGP” chapter of the *Cisco IOS IP Configuration Guide*. For multiprotocol BGP configuration information and examples, refer to the “Configuring Multiprotocol BGP Extensions for IP Multicast” chapter of the *Cisco IOS IP Configuration Guide*. For multiprotocol BGP command descriptions, refer to the “Multiprotocol BGP Extensions for IP Multicast Commands” chapter of the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*.

aggregate-address

To create an aggregate entry in a Border Gateway Protocol (BGP) or multiprotocol BGP database, use the **aggregate-address** command in address family or router configuration mode. To disable this function, 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 the route map used to select the routes to be suppressed.
advertise-map <i>map-name</i>	(Optional) Name of the route map used to select the routes to create AS_SET origin communities.
attribute-map <i>map-name</i>	(Optional) Name of the route map used to set the attribute of the aggregate route.

Defaults

This command is disabled by default.

Command Modes

Address family configuration
Router configuration

Command History

Release	Modification
10.0	This command was introduced.
11.1(20)CC	The nlri unicast , nlri multicast , and nlri unicast multicast keywords were added.
12.0(2)S	The nlri unicast , nlri multicast , and nlri unicast multicast keywords were added.
12.0(7)T	The nlri unicast , nlri multicast , and nlri unicast multicast keywords were removed. Address family configuration mode was added.

Usage Guidelines

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

Using the **aggregate-address** command with no keywords will create an aggregate entry in the BGP or multiprotocol BGP routing table if any more-specific BGP or multiprotocol BGP routes are available that fall in the specified range. The aggregate route will be advertised as coming from your autonomous system and will have 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 the **aggregate-address** command when aggregating many paths, because this route must be continually withdrawn and reupdated 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 also suppresses advertisements of more-specific routes to all neighbors. If you want to suppress only advertisements to certain neighbors, you may use the **neighbor distribute-list** command, with caution. If a more-specific route leaks out, all BGP or multiprotocol BGP routers 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.

Using the **advertise-map** keyword selects specific routes that will be used to build different components of the aggregate route, such as AS_SET or community. This form of the **aggregate-address** command is useful when the components of an aggregate are in separate autonomous systems and you want to create an aggregate with AS_SET, and advertise it back to some of the same autonomous systems. You must remember to omit the specific autonomous system numbers from the AS_SET to prevent the aggregate from being dropped by the BGP loop detection mechanism at the receiving router. IP access lists and autonomous system path access lists **match** clauses are supported.

Using the **attribute-map** keyword allows attributes of the aggregate route to be changed. This form of the **aggregate-address** command is useful when one of the routes forming the AS_SET is configured with an attribute such as the community no-export attribute, which would prevent the aggregate route from being exported. An attribute map route map can be created to change the aggregate attributes.

Examples

In the following example, a BGP aggregate address is created in router configuration mode. 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 65000
aggregate-address 10.0.0.0 255.0.0.0 as-set
```

In the following example, a multiprotocol BGP aggregate address is created in address family configuration mode and applied to the multicast database only using an IP Version 4 address family. More-specific routes are filtered from updates.

```
router bgp 65000
address-family ipv4 multicast
aggregate-address 10.0.0.0 255.0.0.0 summary-only
```

In the following example, a route map called map-one is created matching on an as-path access list. The path advertised for this route will be an AS_SET consisting of elements contained in paths that are matched in the route map.

```
ip as-path access-list 1 deny ^1234_
ip as-path access-list 1 permit .*
!
route-map map-one
match ip as-path 1
!
router bgp 65000
aggregate-address 10.0.0.0 255.0.0.0 as-set advertise-map map-one
```

Related Commands

Command	Description
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
neighbor distribute-list	Distribute BGP neighbor information in an access list.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.

auto-summary (BGP)

To restore the default behavior of automatic summarization of subnet routes into network-level routes, use the **auto-summary** command in address family or router configuration mode. To disable this feature and send subprefix routing information across classful network boundaries, use the **no** form of this command.

auto-summary

no auto-summary

Syntax Description

This command has no arguments or keywords.

Defaults

The behavior of this command is enabled by default (the software summarizes subprefixes to the classful network boundary when crossing classful network boundaries).

Command Modes

Address family configuration

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(7)T	Address family configuration mode was added.

Usage Guidelines

Route summarization reduces the amount of routing information in the routing tables.

By default, BGP does not accept subnets redistributed from Interior Gateway Protocol (IGP). To advertise and carry subnet routes in BGP, use an explicit **network** command or the **no auto-summary** command. If you disable automatic 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.

Examples

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

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

In the following address family configuration mode example, network numbers are not summarized automatically:

```
router bgp 6
 address-family ipv4 unicast
 no auto-summary
```

Related Commands

Command	Description
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.

bgp 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** command in router configuration mode. 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.

Defaults

The Cisco IOS software does not compare MEDs for paths from neighbors in different autonomous systems.

Command Modes

Router configuration

Command History

Release	Modification
11.0	This command was introduced.

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.

Examples

The following example configures the BGP speaker in autonomous system 109 to compare MEDs among alternative paths, regardless of the autonomous system from which the paths are received:

```
router bgp 109
  bgp always-compare-med
```

bgp bestpath as-path ignore

To prevent the router from considering as-path as a factor in the algorithm for choosing a route, use the **bgp bestpath as-path ignore** command in router configuration mode. To allow the router to consider as-path in choosing a route, use the **no** form of this command.

bgp bestpath as-path ignore

no bgp bestpath as-path ignore

Syntax Description This command has no arguments or keywords.

Defaults The router considers as-path in choosing a route.

Command Modes Router configuration

Command History	Release	Modification
	12.0	This command was introduced.

Examples The following example prevents the BGP router from considering as-path as a factor in choosing a route:

```
router bgp 210
  bgp bestpath as-path ignore
```

Related Commands	Command	Description
	show ip bgp ipv4	Displays information about the TCP and BGP connections to neighbors.

bgp bestpath compare-routerid

To compare similar routes received from external BGP (eBGP) peers during the best path selection process and switch the best path to the route with the lowest router ID, use the **bgp bestpath compare-routerid** command in router configuration mode. To return the router to the default setting, use the **no** form of this command.

bgp bestpath compare-routerid

no bgp bestpath compare-routerid

Syntax Description This command has no arguments or keywords.

Defaults Border Gateway Protocol (BGP) does not compare similar paths received from eBGP peers during the best path selection process and switch the best path to the route with the lowest router ID.

Command Modes Router configuration

Command History	Release	Modification
	12.0	This command was introduced.
	12.0 S	This command was introduced.
	12.0 ST	This command was introduced.

Usage Guidelines By default, during the best path selection process, when BGP receives similar routes from eBGP peers (all the attributes are the same except for the router ID), the best path is not switched to the route with the lowest router ID if that route was not the first route received. If the **bgp bestpath compare-routerid** command is enabled, then similar routes are compared and the best path is switched to the route with the lowest router ID.

Examples The following example shows the BGP speaker in autonomous system 500 configured to compare the router IDs of similar paths, regardless of the autonomous system from which the paths are received:

```
router bgp 500
  bgp bestpath compare-routerid
```

Related Commands	Command	Description
	show ip bgp	Displays entries in the BGP routing table.

bgp bestpath med confed

To enable Multi Exit Discriminator (MED) comparison among paths learned from confederation peers, use the **bgp bestpath med confed** command in router configuration mode. To prevent the software from considering the MED attribute in comparing paths, use the **no** form of this command.

bgp bestpath med confed

no bgp bestpath med confed

Syntax Description

This command has no arguments or keywords.

Defaults

The software does not consider the MED attribute when choosing among paths learned from confederation peers.

Command Modes

Router configuration

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

The comparison between MEDs is made only if no external autonomous systems are in the path (an external autonomous system is an autonomous system that is not within the confederation). If an external autonomous system in the path, then the external MED is passed transparently through the confederation, and the comparison is not made.

For example, assume that autonomous system 65000, 65001, 65002, and 65004 are part of the confederation; autonomous system 1 is not; and we are comparing route A with four paths. If the **bgp bestpath med confed** command is enabled, path 1 would be chosen. The fourth path has a lower MED, but it is not involved in the MED comparison because there is an external autonomous system in this path. The following list displays the MED for each autonomous system.

path = 65000 65004, med = 2

path = 65001 65004, med = 3

path = 65002 65004, med = 4

path = 65003 1, med = 1

Examples

The following command enables the BGP router to compare MED values for paths learned from confederation peers:

```
router bgp 210
  bgp bestpath med confed
```

Related Commands

Command	Description
show ip bgp	Displays entries in the BGP routing table.
show ip bgp ipv4	Displays information about the TCP and BGP connections to neighbors.

bgp bestpath med missing-as-worst

To have Cisco IOS software consider a missing Multi Exit Discriminator (MED) attribute in a path as having a value of infinity, making the path without a MED value the least desirable path, use the **bgp bestpath med missing-as-worst** command in router configuration mode. To return the router to the default (assign a value of 0 to the missing MED), use the **no** form of this command.

bgp bestpath med missing-as-worst

no bgp bestpath med missing-as-worst

Syntax Description This command has no arguments or keywords.

Defaults The software assigns a value of 0 to the missing MED, causing the path with the missing MED attribute to be considered the best path.

Command Modes Router configuration

Command History	Release	Modification
	12.0	This command was introduced.

Examples The following example specifies the BGP router to consider a missing MED attribute in a path as having a value of infinity, making this path the least desirable path:

```
router bgp 210
  bgp bestpath med missing-as-worst
```

Related Commands	Command	Description
	show ip bgp	Displays entries in the BGP routing table.
	show ip bgp ipv4	Displays information about the TCP and BGP connections to neighbors.

bgp client-to-client reflection

To restore route reflection from a BGP route reflector to clients, use the **bgp client-to-client reflection** command in address family or router configuration mode. To disable client-to-client reflection, use the **no** form of this command.

bgp client-to-client reflection

no bgp client-to-client reflection

Syntax Description

This command has no arguments or keywords.

Defaults

When a route reflector is configured, the route reflector reflects routes from a client to other clients.

Command Modes

Address family configuration

Router configuration

Command History

Release	Modification
11.1	This command was introduced.
12.0(7)T	Address family configuration mode was added.

Usage Guidelines

By default, the clients of a route reflector are not required to be fully meshed and the routes from a client are reflected to other clients. However, if the clients are fully meshed, route reflection is not required. Use the **no bgp client-to-client reflection** command to disable client-to-client reflection.

Examples

In the following router configuration mode example, the local router is a route reflector. The three neighbors are fully meshed, so client-to-client reflection is disabled.

```
router bgp 5
 neighbor 10.24.95.22 route-reflector-client
 neighbor 10.24.95.23 route-reflector-client
 neighbor 10.24.95.24 route-reflector-client
 no bgp client-to-client reflection
```

In the following address family configuration mode example, the local router is a route reflector. The three neighbors are fully meshed, so client-to-client reflection is disabled.

```
router bgp 5
 address-family ipv4 unicast
 neighbor 10.24.95.22 route-reflector-client
 neighbor 10.24.95.23 route-reflector-client
 neighbor 10.24.95.24 route-reflector-client
 no bgp client-to-client reflection
```

Related Commands	Command	Description
	address-family ipv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
	address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
	bgp cluster-id	Configures the cluster ID if the BGP cluster has more than one route reflector.
	neighbor route-reflector-client	Configures the router as a BGP route reflector and configures the specified neighbor as its client.
	show ip bgp	Displays entries in the BGP routing table.

bgp cluster-id

To configure the cluster ID if the BGP cluster has more than one route reflector, use the **bgp cluster-id** command in router configuration mode. To remove the cluster ID, use the **no** form of this command.

bgp cluster-id *cluster-id*

no bgp cluster-id *cluster-id*

Syntax Description	<i>cluster-id</i> Cluster ID of this router acting as a route reflector; maximum of 4 bytes.
---------------------------	--

Defaults	The router ID of the single route reflector in a cluster
-----------------	--

Command Modes	Router configuration
----------------------	----------------------

Command History	Release	Modification
	11.0	This command was introduced.

Usage Guidelines

Together, a route reflector and its clients form a *cluster*.

Usually a cluster of clients will have a single route reflector. In that case, the cluster is identified by the router ID of the route reflector. In order to increase redundancy and avoid a single point of failure, a cluster might have more than one route reflector. In this case, all route reflectors in the cluster must be configured with the 4-byte cluster ID so that a route reflector can recognize updates from route reflectors in the same cluster.

If the cluster has more than one route reflector, use this command to configure the cluster ID.

Examples

In the following example, the local router is one of the route reflectors serving the cluster. It is configured with the cluster ID to identify the cluster.

```
router bgp 5
 neighbor 198.92.70.24 route-reflector-client
 bgp cluster-id 50000
```

Related Commands	Command	Description
	bgp client-to-client reflection	Restores route reflection from a BGP route reflector to clients.
	neighbor route-reflector-client	Configures the router as a BGP route reflector and configures the specified neighbor as its client.
	show ip bgp	Displays entries in the BGP routing table.

bgp confederation identifier

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

bgp confederation identifier *as-number*

no bgp confederation identifier *as-number*

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

Defaults	No confederation identifier is configured.
-----------------	--

Command Modes	Router configuration
----------------------	----------------------

Command History	Release	Modification
	10.3	This command was introduced.

Usage Guidelines	One way to reduce the internal BGP (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 external BGP (eBGP) sessions, they exchange routing information as if they are iBGP peers. Specifically, the next hop, Multi Exit Discriminator (MED), and local preference information is preserved. The preservation of this information enables you to retain a single Interior Gateway Protocol (IGP) for all the autonomous systems. To the outside world, the confederation looks like a single autonomous system.
-------------------------	--

Examples	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 10.2.3.4 is someone inside your routing domain confederation. Neighbor 10.4.5.6 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 10.2.3.4 remote-as 4002
  neighbor 10.4.5.6 remote-as 510
```

Related Commands

Command	Description
bgp confederation peers	Configures the autonomous systems that belong to the confederation.

bgp confederation peers

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

bgp confederation peers *as-number* [... *as-number*]

no bgp confederation peers *as-number* [... *as-number*]

Syntax Description

<i>as-number</i>	Autonomous system numbers for BGP peers that will belong to the confederation.
------------------	--

Defaults

No BGP peers are identified as belonging to the confederation.

Command Modes

Router configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

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

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 to which the autonomous systems belong.

Examples

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 Commands

Command	Description
bgp confederation identifier	Specifies a BGP confederation identifier.

bgp dampening

To enable BGP route dampening or change various BGP route dampening factors, use the **bgp dampening** command in address family or router configuration mode. To disable the function or restore the default values, use the **no** form of this command.

bgp dampening [*half-life reuse suppress max-suppress-time*] [**route-map** *map-name*]

no bgp dampening [*half-life reuse suppress max-suppress-time*] [**route-map** *map-name*]

Syntax Description

<i>half-life</i>	(Optional) Time (in minutes) after which a penalty is decreased. Once the route has been assigned a penalty, the penalty is decreased by half after the half-life period (which is 15 minutes by default). The process of reducing the penalty happens every 5 seconds. The range of the half-life period is 1 to 45 minutes. The default is 15 minutes.
<i>reuse</i>	(Optional) Reuse values based on accumulated penalties. If the penalty for a flapping route decreases enough to fall below this value, the route is unsuppressed. The process of unsuppressing routes occurs at 10-second increments. The range of the reuse value is from 1 to 20000; the default is 750.
<i>suppress</i>	(Optional) A route is suppressed when its penalty exceeds this limit. The range is from 1 to 20000; the default is 2000.
<i>max-suppress-time</i>	(Optional) Maximum time (in minutes) a route can be suppressed. The range is from 1 to 20000; the default is 4 times the <i>half-life</i> . If the <i>half-life</i> value is allowed to default, the maximum suppress time defaults to 60 minutes. When the <i>max-suppress-time</i> is configured, the maximum penalty will never be exceeded, regardless of the number of times that the prefix dampens. The maximum penalty is computed with the following formula: Max penalty = reuse-limit * 2 ^(maximum suppress time/half time)
route-map <i>map-name</i>	(Optional) Name of route map that controls where BGP route dampening is enabled.

Defaults

This command is disabled by default

half-life: 15 minutes

reuse: 750

suppress: 2000

max-suppress-time: 4 times *half-life*

Command Modes

Address family configuration

Router configuration

Command History

Release	Modification
11.0	This command was introduced.
12.0(7)T	Address family configuration mode was added.

Usage Guidelines

If this command is used with no arguments, it enables BGP route dampening. The *half-life*, *reuse*, *suppress*, and *max-suppress-time* arguments are position-dependent. Therefore, if any of these arguments are issued, they must all be specified.

When BGP dampening is configured and a prefix is withdrawn, BGP considers the withdrawn prefix as a flap and increases the penalty by a 1000. If BGP receives an attribute change, BGP increases the penalty by 500. If then the prefix has been withdrawn, BGP keeps the prefix in the BGP table as a history entry. If the prefix has not been withdrawn by the neighbor and BGP is not using this prefix, the prefix is marked as dampened. Dampened prefixes are not used in the BGP decision process and not installed to the routing table.

Examples

The following router configuration mode example sets the half life to 30 minutes, the reuse value to 1500, the suppress value to 10000, and the maximum suppress time to 120 minutes:

```
router bgp 5
  bgp dampening 30 1500 10000 120
```

The following address family configuration mode example sets the half life to 30 minutes, the reuse value to 1500, the suppress value to 10000, and the maximum suppress time to 120 minutes:

```
router bgp 5
  address-family ipv4 multicast
  bgp dampening 30 1500 10000 120
```

Related Commands

Command	Description
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
clear ip bgp dampening	Clears BGP route dampening information and unsuppresses the suppressed routes.
clear ip bgp flap-statistics	Clears BGP flap statistics.
show ip bgp dampened-paths	Displays BGP dampened routes.
show ip bgp flap-statistics	Displays BGP flap statistics.

bgp default ipv4-unicast

To enable the IP version 4 (IPv4) unicast address family on all neighbors, use the **bgp default ipv4-unicast** command in address family or router configuration mode. To disable the IPv4 unicast address family on all neighbors, use the **no** form of this command.

bgp default ipv4-unicast

no bgp default ipv4-unicast

Syntax Description This command has no arguments or keywords.

Defaults This command is disabled by default.

Command Modes Address family
Router configuration

Command History	Release	Modification
	12.0(5)T	This command was introduced.

Usage Guidelines Use the **neighbor activate** address family configuration command for each neighbor you want to run the **bgp default ipv4-unicast** command for under the IPv4 unicast address family.

Examples The following example enables IP version 4 unicast address family on all neighbors:

```
bgp default ipv4-unicast
```

Related Commands	Command	Description
	neighbor activate	Enables the exchange of information with a neighboring router.

bgp default local-preference

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

bgp default local-preference *number*

no bgp default local-preference *number*

Syntax Description	<i>number</i>	Local preference value from 0 to 4294967295. Higher is more preferred.
---------------------------	---------------	--

Defaults	Local preference value of 100
-----------------	-------------------------------

Command Modes	Router configuration
----------------------	----------------------

Command History	Release	Modification
	10.0	This command was introduced.

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 and access servers in the local autonomous system.
-------------------------	--

Examples	The following example raises the default local preference value from the default of 100 to 200: <pre>router bgp 200 bgp default local-preference 200</pre>
-----------------	---

Related Commands	Command	Description
	set local-preference	Specifies a preference value for the autonomous system path.

bgp deterministic-med

To have Cisco IOS software enforce the deterministic comparison of the Multi Exit Discriminator (MED) variable between all paths received from the same autonomous system, use the **bgp deterministic-med** command in router configuration mode. To disable the comparison, use the **no** form of this command.

bgp deterministic med

no bgp deterministic med

Syntax Description This command has no arguments or keywords.

Defaults The software does not enforce the deterministic comparison of the MED variable between all paths received from the same autonomous system.

Command Modes Router configuration
Address-family configuration

Release	Modification
11.1	This command was introduced.

Usage Guidelines After the **bgp always-compare-med** command is configured, all paths for the same prefix that are received from different neighbors, which are in the same autonomous system, will be grouped together and sorted by the ascending MED value (received-only paths are ignored and not grouped or sorted). The best path selection algorithm will then pick the best paths using the existing rules; the comparison is made on a per neighbor autonomous system basis and then global basis. The grouping and sorting of paths occurs immediately after this command is entered. For correct results, all routers in the local autonomous system must have this command enabled (or disabled).

Examples The following example specifies that the BGP router compare MED variables when choosing among routes advertised by the same subautonomous system within a confederation:

```
Router(config)# router bgp 204  
Router(config-router)# bgp deterministic-med
```

The following example **show ip bgp** command output illustrates how route selection is affected by the configuration of the **bgp deterministic-med** command. The order in which routes are received affects how routes are selected for best path selection when the **bgp deterministic-med** command is not enabled.

The following sample output from the **show ip bgp** command shows three paths that are received for the same prefix (10.100.0.0), and the **bgp deterministic-med** command is not enabled:

```
router# show ip bgp 10.100.0.0
BGP routing table entry for 10.100.0.0/16, version 40
Paths: (3 available, best #3, advertised over IBGP, EBGP)
 109
   192.168.43.10 from 192.168.43.10 (192.168.43.1)
      Origin IGP, metric 0, localpref 100, valid, internal
 2051
   192.168.43.22 from 192.168.43.22 (192.168.43.2)
      Origin IGP, metric 20, localpref 100, valid, internal
 2051
   192.168.43.3 from 192.168.43.3 (10.4.1.1)
      Origin IGP, metric 30, valid, external, best
```

If the **bgp deterministic-med** command is not enabled on the router, the route selection can be affected by the order in which the routes are received. Consider the following scenario in which a router received three paths for the same prefix:

The **clear ip bgp *** command is entered to clear all routes in the local routing table.

```
Router# clear ip bgp *
```

The **show ip bgp** command is issued again after the routing table has been repopulated. Note that the order of the paths changed after clearing the BGP session. The results of the selection algorithm also changed. This occurred because the order in which the paths were received was different for the second session.

```
Router# show ip bgp 10.100.0.0
BGP routing table entry for 10.100.0.0/16, version 2
Paths: (3 available, best #3, advertised over EBGP)
 109 192.168.43.10 from 192.168.43.10 (192.168.43.1)
      Origin IGP, metric 0, localpref 100, valid, internal
 2051
   192.168.43.3 from 192.168.43.3 (10.4.1.1)
      Origin IGP, metric 30, valid, external
 2051
   192.168.43.22 from 192.168.43.22 (192.168.43.2)
      Origin IGP, metric 20, localpref 100, valid, internal, best
```

If the **bgp deterministic-med** command is enabled, then the result of the selection algorithm will always be the same, regardless of the order in which the paths are received by the local router. The following output is always generated when the **bgp deterministic-med** command is entered on the local router in this scenario:

```
Router# show ip bgp 10.100.0.0
BGP routing table entry for 10.100.0.0/16, version 15
Paths: (3 available, best #1, advertised over EBGP)
 109
   192.168.43.10 from 192.168.43.10 (192.168.43.1)
      Origin IGP, metric 0, localpref 100, valid, internal, best 3
 192.168.43.22 from 192.168.43.22 (192.168.43.2)
      Origin IGP, metric 20, localpref 100, valid, internal 3
 192.168.43.3 from 192.168.43.3 (10.4.1.1)
      Origin IGP, metric 30, valid, external
```

Related Commands

Command	Description
clear ip bgp	Resets a BGP connection or session.

show ip bgp	Displays entries in the BGP routing table.
show ip bgp neighbors	Displays information about the TCP and BGP connections to neighbors.

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** command in address family or router configuration mode. To disable this function, 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.

Defaults The behavior of this command is enabled by default.

Command Modes Address family configuration
Router configuration

Command History	Release	Modification
	10.0	This command was introduced.
	12.0(7)T	Address family configuration mode was added.

Examples The following example disables the automatic resetting of BGP sessions in router configuration mode:

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

The following example disables the automatic resetting of BGP sessions in address family configuration mode:

```
router bgp 109
 address-family ipv4 unicast
 no bgp fast-external-fallover
```

Related Commands	Command	Description
	address-family ipv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.

bgp log-neighbor-changes

To enable logging of BGP neighbor resets, use the **bgp log-neighbor-changes** command in address family or router configuration mode. To disable the logging of changes in BGP neighbor adjacencies, use the **no** form of this command.

bgp log-neighbor-changes

no bgp log-neighbor-changes

Syntax Description

This command has no arguments or keywords.

Defaults

BGP neighbor changes are logged.

Command Modes

Address family configuration
Router configuration

Command History

Release	Modification
11.1 CC	This command was introduced.
12.0	This command was introduced.
12.0(7)T	Address family configuration mode was added.
12.0(1)	BGP neighbor changes are logged by default.

Usage Guidelines

The **bgp log-neighbor-changes** command enables logging of BGP neighbor status changes (up or down) and resets for troubleshooting network connectivity problems and measuring network stability. Unexpected neighbor resets might indicate high error rates or high packet loss in the network and should be investigated.

Using the **bgp log-neighbor-changes** command to enable status change message logging does not cause a substantial performance impact, unlike, for example, enabling per BGP update debugging. If the UNIX syslog facility is enabled, messages are sent to the UNIX host running the syslog daemon so that the messages can be stored and archived. If the UNIX syslog facility is not enabled, the status change messages are retained in the internal buffer of the router, and are not stored to disk. You can set the size of this buffer, which is dependent upon the available RAM, using the **logging buffered** command.

The neighbor status change messages are not tracked if the **bgp log-neighbor-changes** command is not enabled, except for the reset reason, which is always available as output of the **show ip bgp neighbors** command.

The **eigrp log-neighbor-changes** command enables logging of Enhanced IGRP (EIGRP) neighbor adjacencies, but messages for BGP neighbors are logged only if they are specifically enabled with the **bgp log-neighbor-changes** command.

Use the **show logging** command to display the log for the BGP neighbor changes.

Examples

The following example logs neighbor changes for BGP in router configuration mode:

```
bgp router 100
  bgp log-neighbor-changes
```

The following example logs neighbor changes for BGP in address family configuration mode:

```
bgp router 100
  address-family ipv4 unicast
    bgp log-neighbor-changes
```

Related Commands

Command	Description
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
eigrp log-neighbor-changes	Enables the logging of neighbor adjacency changes to monitor the stability of the routing system and to help detect problems.
logging buffered	Logs messages to an internal buffer.
show ip bgp ipv4	Displays information about the TCP and BGP connections to neighbors.
show ip bgp neighbors	Displays information about BGP neighbors.
show logging	Displays the state of logging (syslog).

bgp maxas-limit

To configure Border Gateway Protocol (BGP) to discard routes that have a number of as-path segments that exceed the specified value, use the **bgp maxas-limit** command in router configuration mode. To return the router to default operation, use the **no** form of this command.

bgp maxas-limit *number*

no bgp maxas-limit

Syntax Description	<i>number</i>	Specifies the number of autonomous system segments. The value that can be entered for this argument is a number from 1 to 2000.
---------------------------	---------------	---

Defaults The default value in Cisco IOS software for the *number* argument is 75.

Command Modes Router configuration

Command History	Release	Modification
	12.2	This command was introduced.
	12.0(17)S	This command was integrated into Cisco IOS Release 12.0(17)S.

Usage Guidelines The **bgp maxas-limit** command is used to limit the number of as-path segments that are permitted in inbound routes. If a route is received with an as-path segment that exceeds the configured limit, the BGP routing process will discard the route.

Examples In the following example, the maximum as-path segment length is set to 30:

```
Router(config)# router bgp 40000
Router(config-router-af)# bgp maxas-limit 30
```

Related Commands	Command	Description
	clear ip bgp	Resets a BGP connection or session.

bgp redistribute-internal

To allow the redistribution of iBGP routes into an interior gateway protocol such as IS-IS or OSPF, use the **bgp redistribute-internal** command in router configuration mode. To remove the **bgp redistribute-internal** command from the configuration file and restore the system to its default condition where the software does not allow the redistribution of iBGP routes into Interior Gateway Protocols (IGPs), use the **no** form of this command.

bgp redistribute-internal

no bgp redistribute-internal

Syntax Description This command has no arguments or keywords.

Defaults By default iBGP routes are not redistributed into IGPs.

Command Modes Router configuration

Command History	Release	Modification
	12.1	This command was introduced.

Usage Guidelines Use of the **bgp redistribute-internal** command requires the **clear ip bgp** command to be issued to reset BGP connections.



Caution

Redistributing iBGP routes into IGPs may cause routing loops to form within an autonomous system. Use this command with caution.

Examples The following example shows iBGP routes being redistributed into OSPF:

```
router ospf 300
 redistribute bgp 200
!
router bgp 200
 bgp redistribute-internal
!
clear ip bgp *
```

Related Commands	Command	Description
	clear ip bgp	Resets a BGP connection or session.

bgp router-id

To configure a fixed router ID for a BGP-speaking router, use the **bgp router-id** command in router configuration mode. To remove the **bgp router-id** command from the configuration file and restore the default value of the router ID, use the **no** form of this command.

bgp router-id *ip-address*

no bgp router-id *ip-address*

Syntax Description

<i>ip-address</i>	IP address of the router.
-------------------	---------------------------

Defaults

The router ID is set to the IP address of a loopback interface if one is configured. If no virtual interfaces are configured, the highest IP address is configured for a physical interface on that router. Peering sessions will be reset if the router ID is changed.

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Use this command to configure a fixed router ID as an identifier of the router running BGP. A loopback interface, if one is configured, is more effective than a fixed interface as an identifier because there is no physical link to go down.

Examples

The following example shows the local router configured with the router ID of 192.168.70.24:

```
router bgp 100
  no synchronization
  bgp router-id 192.168.70.24
```

Related Commands

Command	Description
show ip bgp	Displays entries in the BGP routing table.

bgp rr-group

To create a route-reflector group and enable automatic inbound filtering for VPN version 4 (VPNv4) updates based on the allowed route target (RT) extended communities, use the **bgp rr-group** command in address family configuration mode. To disable a route-reflector group or route reflector, use the **no** form of this command.

bgp rr-group *extcom-list-number*

no bgp rr-group

Syntax Description

<i>extcom-list-number</i>	Number of a specific extended community-list that will be supported by the route-reflector group. The range of extended community-list numbers that can be specified is from 1 to 199. However, only one extended community-list is specified with the <i>extcom-list-number</i> argument.
---------------------------	--

Defaults

This command has no default behavior.

Command Modes

Address family configuration

Command History

Release	Modification
12.1	This command was introduced.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S. The maximum number of extended community-lists that can be supported by a route-reflector group was changed from 199 to 500.

Usage Guidelines

The **bgp rr-group** command can be used with the **ip extcommunity-list** command. The **ip extcommunity-list** command is used to create an extended community-list and specify a list of extended community RTs. Only extended community-lists are supported.

Examples

The following example configures a route-reflector group that will accept extended community-list number 500:

```
router bgp 101
 address-family vpnv4
  bgp rr-group 500
```

Related Commands

Command	Description
ip extcommunity-list	Creates an extended community access list.

bgp suppress-inactive

To keep routes that are not installed in the routing information base (RIB) from being advertised to peers, use the **bgp suppress-inactive** command in address family or router configuration mode.

bgp suppress-inactive

no bgp suppress inactive

Syntax Description This command has no keywords or arguments.

Defaults This command is disabled by default.

Command Modes
Address family
Router configuration

Command History	Release	Modification
	12.2T	This command was introduced.

Usage Guidelines This command is a toggle. Use the **bgp suppress-inactive** command to prevent routes that are not installed in the RIB from being advertised to peers. Use the **no bgp suppress-inactive** command to make BGP ignore RIB failures when advertising routes to peers.

Examples In the following example, the **bgp suppress-inactive** command is configured:

```
Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# router bgp 1

Router(config-router)# bgp suppress-inactive
```

Related Commands	Command	Description
	clear ip bgp	Resets a BGP connection using BGP soft reconfiguration.
	show ip bgp rib-failure	Display BGP routes that failed to install in the RIB table.

clear ip bgp

To reset a BGP connection using BGP soft reconfiguration, use the **clear ip bgp** command in privileged EXEC mode at the system prompt.

```
clear ip bgp { * | neighbor-address | peer-group-name } [soft [in | out]]
```

Syntax Description

*	Specifies that all current BGP sessions will be reset.
<i>neighbor-address</i>	Specifies that only the identified BGP neighbor will be reset.
<i>peer-group-name</i>	Specifies that the specified BGP peer group will be reset.
soft	(Optional) Soft reset. Does not reset the session.
in out	(Optional) Triggers inbound or outbound soft reconfiguration. If the in or out option is not specified, both inbound and outbound soft reset is triggered.

Defaults

No reset is initiated.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.0(6)T	The dynamic inbound soft reset capability was added.
12.0(2)S	The dynamic inbound soft reset capability was added.

Usage Guidelines

You can reset inbound routing table updates dynamically or by generating new updates using stored update information. Using stored update information required additional memory for storing the updates.

To reset inbound routing table updates dynamically, all BGP routers must support the route refresh capability. To determine whether a BGP router supports this capability, use the **show ip bgp neighbors** command. If a router supports the route refresh capability, the following message is displayed:

```
Received route refresh capability from peer.
```

If all BGP routers support the route refresh capability, use the **clear ip bgp** { * | *address* | *peer-group-name* } **in** command. You need not use the **soft** keyword, because soft reset is automatically assumed when the route refresh capability is supported.

To generate new inbound updates from stored update information (rather than dynamically) without resetting the BGP session, you must preconfigure the local BGP router using the **neighbor soft-reconfiguration inbound** command. This preconfiguration causes the software to store all received updates without modification regardless of whether an update is accepted by the inbound policy. Storing updates is memory intensive and should be avoided if possible.

Outbound BGP soft configuration has no memory overhead and does not require any preconfiguration. You can trigger an outbound reconfiguration on the other side of the BGP session to make the new inbound policy take effect.

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 to BGP-related route maps

Examples

The following example clears the inbound session with the neighbor 10.108.1.1 without resetting the session:

```
Router# clear ip bgp 10.108.1.1 soft in
```

The following example clears the outbound session with the peer group named corp without resetting the session:

```
Router# clear ip bgp corp soft out
```

Related Commands

Command	Description
neighbor soft-reconfiguration	Configures the Cisco IOS software to start storing updates.
show ip bgp	Displays entries in the BGP routing table.

clear ip bgp dampening

To clear BGP route dampening information and unsuppress the suppressed routes, use the **clear ip bgp dampening** command in privileged EXEC mode.

```
clear ip bgp dampening [ip-address network-mask]
```

Syntax Description		
<i>ip-address</i>	(Optional) IP address of the network about which to clear dampening information.	
<i>network-mask</i>	(Optional) Network mask applied to the <i>ip-address</i> argument.	

Command Modes	Privileged EXEC
---------------	-----------------

Command History	Release	Modification
	11.0	This command was introduced.

Examples

The following example clears route dampening information about the route to network 192.168.0.0 and unsuppresses its suppressed routes. When the address and mask arguments are not specified, the **clear ip bgp dampening** command clears route dampening information for the entire BGP routing table.

```
Router# clear ip bgp dampening 192.168.0.0 255.255.0.0
```

Related Commands	Command	Description
	bgp dampening	Enables BGP route dampening or changes various BGP route dampening factors.
	show ip bgp dampened-paths	Displays BGP dampened routes.

clear ip bgp external

To clear external Border Gateway Protocol (eBGP) peers, use the **clear ip bgp external** command in privileged EXEC mode.

```
clear ip bgp external [in | out]
```

```
clear ip bgp external [soft [in | out]]
```

```
clear ip bgp external {ipv4 | ipv6} {multicast | unicast [in | out | soft]}
```

```
clear ip bgp external [vpn4 unicast {in | out | soft}]
```

Syntax Description	in out	(Optional) Triggers inbound or outbound soft reconfiguration.
	soft	(Optional) Triggers soft reconfiguration.
	ipv4 ipv6 vpn4	(Optional) Triggers reset of IPv4, IPv6, or VPNv4 address family session.
	multicast	(Optional) Triggers reset of IPv4 or IPv6 multicast address family session.
	unicast	(Optional) Triggers reset of IPv4, IPv6, or VPNv4 unicast family session.

Defaults A reset is not initiated.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.0(2)S	This command was introduced.

Usage Guidelines Using the **clear ip bgp external** command without the **soft** keyword will reset the session.

Examples The following example clears an inbound session with the eBGP peers:

```
Router# clear ip bgp external in
```

or

```
Router# clear ip bgp external soft in
```

The following examples clear an outbound address family IPv4 multicast session with the eBGP peers:

```
Router# clear ip bgp external ipv4 multicast out
```

Related Commands	Command	Description
	clear ip bgp	Resets a BGP connection or session.

■ `clear ip bgp external`

neighbor soft-reconfiguration	Configures the Cisco IOS software to start storing updates.
show ip bgp	Displays entries in the BGP routing table.

clear ip bgp flap-statistics

To clear BGP flap statistics, use the **clear ip bgp flap-statistics** command in privileged EXEC mode.

```
clear ip bgp ip-address flap-statistics [{regexp regexp} | {filter-list list-name} | {ip-address
network-mask}]
```

```
clear ip bgp [ip-address] flap-statistics
```

Syntax Description	
<i>ip-address</i>	(Optional) Clears flap statistics for a single entry at this IP address. If this argument is placed before flap-statistics , the router clears flap statistics for all paths from the neighbor at this address.
regexp <i>regexp</i>	(Optional) Clears flap statistics for all the paths that match the regular expression.
filter-list <i>list-name</i>	(Optional) Clears flap statistics for all the paths that pass the access list.
<i>network-mask</i>	(Optional) Network mask applied to the <i>address</i> argument.

Defaults No statistics are cleared.

Command Modes Privileged EXEC

Command History	Release	Modification
	11.0	This command was introduced.

Usage Guidelines If no arguments or keywords are specified, the router will clear BGP flap statistics for all routes. The flap statistics for a route are also cleared when a BGP peer is reset. Although the reset withdraws the route, no penalty is applied in this instance even though route flap dampening is enabled.

Examples The following example clears all of the flap statistics for paths that pass filter list 3:

```
Router# clear ip bgp flap-statistics filter-list 3
```

Related Commands	Command	Description
	bgp dampening	Enables BGP route dampening or changes various BGP route dampening factors.

clear ip bgp peer-group

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

clear ip bgp peer-group *tag*

Syntax Description	<i>tag</i>	Name of the BGP peer group to clear.
---------------------------	------------	--------------------------------------

Defaults	No BGP peer group members are cleared.
-----------------	--

Command Modes	Privileged EXEC
----------------------	-----------------

Command History	Release	Modification
	11.0	This command was introduced.

Examples	The following example clears all members from the BGP peer group named internal:
-----------------	--

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

Related Commands	Command	Description
	neighbor peer-group (assigning members)	Configures a BGP neighbor to be a member of a peer group.

clear ip prefix-list

To reset the hit count of the prefix list entries, use the **clear ip prefix-list** command in privileged EXEC mode.

```
clear ip prefix-list [prefix-list-name] [network/length]
```

Syntax Description		
<i>prefix-list-name</i>	(Optional) The name of the prefix list from which the hit count is to be cleared.	
<i>network/length</i>	(Optional) The network number and length (in bits) of the network mask. The slash mark is required.	

Defaults Does not clear the hit count.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.0	This command was introduced.

Usage Guidelines The hit count is a value indicating the number of matches to a specific prefix list entry.

Examples The following example clears the hit count from the prefix list entries for the prefix list named `first_list` that match the network mask `10.0.0.0/8`:

```
Router# clear ip prefix-list first_list 10.0.0.0/8
```

Related Commands	Command	Description
	<code>distribute-list in (IP)</code>	Filters networks received in updates.
	<code>distribute-list out</code>	Suppresses networks from being advertised in updates.
	<code>ip prefix-list</code>	Creates an entry in a prefix list.
	<code>ip prefix-list description</code>	Adds a text description of a prefix list.
	<code>ip prefix-list sequence-number</code>	Enables the generation of sequence numbers for entries in a prefix list.
	<code>redistribute (IP)</code>	Redistributes routes from one routing domain into another routing domain.
	<code>show ip bgp regexp</code>	Displays information about a prefix list or prefix list entries.

default-information originate (BGP)

To control the redistribution of a protocol or network into the BGP, use the **default-information originate** command in address family or router configuration mode. To disable this function, use the **no** form of this command.

default-information originate

no default-information originate

Syntax Description This command has no arguments or keywords.

Defaults This command is disabled by default.

Command Modes Address family configuration
Router configuration

Command History	Release	Modification
	10.0	This command was introduced.
	12.0(7)T	Address family configuration mode was added.

Usage Guidelines The **default-information originate** command should be used if the network operator needs to control the redistribution of default routes. Using the **default-information originate** command in BGP is similar to using the **network** command. However, to achieve the same result as configuring the **network** command with the route 0.0.0.0, the **default-information originate** command requires an explicit redistribution of the route 0.0.0.0. The **network** command requires only that route 0.0.0.0 is specified in the Interior Gateway Protocol (IGP) routing table. For this reason, the **network** command is preferred for redistributing default routes and protocols into BGP.

Examples The following address family configuration mode example configures BGP to redistribute OSPF into BGP:

```
router bgp 164
  address-family ipv4 unicast
  default-information originate
  redistribute ospf 109
```

The following router configuration mode example configures BGP to redistribute OSPF into BGP:

```
router bgp 164
  default-information originate
  redistribute ospf 109
```

Related Commands

Command	Description
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
neighbor ebgp-multihop	Accepts and attempts BGP connections to external peers residing on networks that are not directly connected.
network (BGP and multiprotocol BGP)	Specifies the list of networks for the BGP routing process.
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.

default-metric (BGP)

To set a default metric for routes redistributed into Border Gateway Protocol (BGP), use the **default-metric** command in address family or router configuration mode. To remove the configured value and return BGP to default operation, use the **no** form of this command.

default-metric *number*

no default-metric *number*

Syntax Description

<i>number</i>	Default metric value applied to the redistributed route. The range of values for this argument is from 1 to 4294967295.
---------------	---

Defaults

The following is default behavior if this command is not configured or if the **no** form of this command is entered:

- The metric of redistributed interior gateway protocol (IGP) routes is set to a value that is equal to the interior BGP (iBGP) metric.
- The metric of redistributed connected and static routes is set to 0.

When this command is enabled, the metric for redistributed connected routes is set to 0.

Command Modes

Address family configuration
Router configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(7)T	Address family configuration mode support was added.

Usage Guidelines

The **default-metric** command is used to set the metric value for routes redistributed into BGP with the **redistribute** command. A default metric can be configured to solve the problem of redistributing routes with incompatible metrics. Assigning the default metric will allow redistribution to occur.

This value is the Multi Exit Discriminator (MED) that is evaluated by BGP during the best path selection process. The MED is a non-transitive value that is processed only within the local autonomous system and adjacent autonomous systems. The default metric is not set if the received route has a MED value.



Note

When enabled, the **default-metric** command applies a metric value of 0 to redistributed connected routes. The **default-metric** command does not override metric values that are applied with the **redistribute** command.

Examples

In the following example, a metric of 1024 is set for routes redistributed into BGP from OSPF:

```
Router(config)# router bgp 50000  
Router(config-router)# address-family ipv4 unicast  
Router(config-router-af)# default-metric 1024  
Router(config-router-af)# redistribute ospf 10  
Router(config-router-af)# end
```

Related Commands

Command	Description
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.

distance bgp

To allow the use of external, internal, and local administrative distances that could be a better route than other external, internal, or local routes to a node, use the **distance bgp** command in address family or router configuration mode. 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

<i>external-distance</i>	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.
<i>internal-distance</i>	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.
<i>local-distance</i>	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.

Defaults

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

Command Modes

Address family configuration
 Router configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(7)T	Address family configuration mode was added.

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 a positive integer from 1 to 255. In general, the higher the value, the lower the trust rating. An administrative distance of 255 means the routing information source cannot be trusted at all and should be ignored.

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 (eBGP), or if some internal routes should be preferred by BGP.

**Caution**

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.

The **distance bgp** command replaces the **distance mbgp** command.

Examples

In the following router configuration mode example, internal routes are known to be preferable to those learned through the Interior Gateway Protocol (IGP), so the administrative distance values are set accordingly:

```
router bgp 109
 network 10.108.0.0
 neighbor 192.168.6.6 remote-as 123
 neighbor 172.16.1.1 remote-as 47
 distance bgp 20 20 200
```

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

```
router bgp 109
 neighbor 192.168.6.6 remote-as 123
 neighbor 172.16.1.1 remote-as 47
 address family ipv4 multicast
 network 10.108.0.0
 distance bgp 20 20 200
 neighbor 192.168.6.6 activate
 neighbor 172.16.1.1 activate
```

Related Commands

Command	Description
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.

distribute-list in (BGP)

To filter routes or networks received in incoming Border Gateway Protocol (BGP) updates, use the **distribute-list in** command in router configuration mode. To delete the distribute list and remove it from the running configuration file, use the **no** form of this command.

distribute-list *acl-number* | **prefix** *list-name* **in**

no distribute-list *acl-number* | **prefix** *list-name* **in**

Syntax Description

<i>acl-number</i>	IP access list number. The access list defines which networks are to be received and which are to be suppressed in routing updates.
prefix <i>list-name</i>	Name of a prefix list. The list defines which networks are to be received and which are to be suppressed in routing updates, based upon matching prefixes in the prefix list.



Note

Interface type and number arguments may be displayed in the CLI depending on the installed version of Cisco IOS software. However, the interface arguments are not support in any software release.

Defaults

If this command is configured without a predefined access list, the distribute list will default to permitting all traffic.

Command Modes

Router configuration



Note

The **distribute-list in** command can be entered in address family configuration mode. However, address family configuration is not recommended and not supported.

Command History

Release	Modification
10.0	This command was introduced.
11.2	The <i>acl-number</i> arguments was added.
12.0	The prefix <i>list-name</i> argument was added.

Usage Guidelines

The **distribute-list in** command is used to filter incoming BGP updates. An access list must be defined prior to configuration of this command. In addition to access lists, prefix list can be used to filter based upon the prefix length, making it possible to filter either on the prefix list, the gateway, or both for incoming updates. The session must be reset with the **clear ip bgp** command before the distribute list will take effect. To suppress networks from being advertised in updates, use the **distribute-list out** command.

**Note**

We recommend that you use IP prefix lists (configured with the **ip prefix-list** command in global configuration mode) instead of distribute lists. IP prefix lists provide improved performance and are simpler to configure. Distribute list configuration will be removed from the CLI at a future date.

**Note**

Prefix lists and access lists are mutually exclusive when configuring a distribute list. We recommend that you do not use both the *prefix-list* and *access-list-name* arguments with the **distribute-list in** command.

Examples

In the following example, a prefix list and distribute list are defined to configure the BGP routing process to accept traffic from only network 192.168.1.0 and network 10.108.0.0. An inbound route refresh is initiated to activate the distribute-list.

```
Router(config)# ip prefix-list RED deny 0.0.0.0/0 le 32
Router(config)# ip prefix-list RED permit 10.108.0.0/16
Router(config)# ip prefix-list RED permit 192.168.1.0/24
Router(config)# !
Router(config)# router bgp 50000
Router(config-router)# network 10.108.0.0
Router(config-router)# distribute-list prefix RED in
Router(config-router)# end
Router# clear ip bgp in
```

In the following example, an access list and a distribute list are defined to configure the BGP routing process to accept traffic from only network 192.168.1.0 and network 10.108.0.0. An inbound route refresh is initiated to activate the distribute-list.

```
Router(config)# access-list 1 permit 192.168.1.0
Router(config)# access-list 1 permit 10.108.0.0
Router(config)# access-list 1 deny 0.0.0.0 255.255.255.255
Router(config)# !
Router(config)# router bgp 50000
Router(config-router)# network 10.108.0.0
Router(config-router)# distribute-list 1 in
Router(config-router)# end
Router# clear ip bgp in
```

Related Commands

Command	Description
access-list	Defines an IP access list.
clear ip bgp	Resets a BGP connection or session.
distribute-list out (BGP)	Suppresses networks from being advertised in outbound BGP updates.
ip prefix-list	Creates an entry in a prefix list.
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.

distribute-list out (BGP)

To suppress networks from being advertised in outbound Border Gateway Protocol (BGP) updates, use the **distribute-list out** command in router configuration mode. To delete the distribute list and remove it from the running configuration file, use the **no** form of this command.

distribute-list *acl-number* | **prefix** *list-name* **out** [*protocol process-number* | **connected** | **static**]

no distribute-list *acl-number* | **prefix** *list-name* **out** [*protocol process-number* | **connected** | **static**]

Syntax Description

<i>acl-number</i>	IP access list number. The access list defines which networks are to be received and which are to be suppressed in routing updates.
prefix <i>list-name</i>	Name of a prefix list. The list defines which networks are to be received and which are to be suppressed in routing updates, based upon matching prefixes in the prefix list.
<i>protocol process-number</i>	Specifies the routing protocol to apply the distribution list. BGP, EIGRP, OSPF, and RIP are supported. The process number is entered for all routing protocols, except RIP. The process number is a value from 1 to 65535.
connected	Specifies peers and networks learned through connected routes.
static	Specifies peers and networks learned through static routes.



Note

Interface type and number arguments may be displayed in the CLI depending on the installed version of Cisco IOS software. However, the interface arguments are not support in any software release.

Defaults

If this command is configured without a predefined access list, the distribute list will default to permitting all traffic.

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
11.2	The <i>acl-number</i> argument was added.
12.0	The prefix <i>list-name</i> argument was added.

Usage Guidelines

The **distribute-list out** command is used to filter outbound BGP updates. An access list must be defined prior to configuration of this command. In addition to access lists, prefix list can be used to filter based upon the prefix length, making it possible to filter either on the prefix list, the gateway, or both for incoming updates. The session must be reset with the **clear ip bgp** command before the distribute list will take effect. To filter routes that are received in inbound updates, use the **distribute-list in** command.

Entering a *protocol* and/or *process-number* arguments causes the distribute list to be applied to only routes derived from the specified routing process. Addresses not specified in the distribute-list command will not be advertised in outgoing routing updates after a distribute list is configured.

**Note**

We recommend that you use IP prefix lists (configured with the [ip prefix-list](#) command in global configuration mode) instead of distribute lists. IP prefix lists provide improved performance and are simpler to configure. Distribute list configuration will be removed from the CLI at a future date.

**Note**

Prefix lists and access lists are mutually exclusive when configuring distribute lists. We recommend that you do not use both the *prefix-list* and *access-list-name* arguments with the **distribute-list out** command.

Examples

In the following example, an access list and a distribute list are defined to configure the BGP routing process to advertise only network 192.168.0.0. An outbound route refresh is initiated to activate the distribute-list.

```
Router(config)# access-list 1 permit 192.168.0.0 0.0.255.255
Router(config)# access-list 1 deny 0.0.0.0 255.255.255.255
Router(config)# !
Router(config)# router bgp 50000
Router(config-router)# distribute-list 1 out
Router(config-router)# end
Router# clear ip bgp out
```

Related Commands

Command	Description
access-list	Defines an IP access list.
clear ip bgp	Resets a BGP connection or session.
distribute-list in (BGP)	Filters routes and networks received in updates.
ip prefix-list	Creates an entry in a prefix list.
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.

export map

To configure an export route map for a VRF, use the **export map** command in VRF configuration mode.

export map *route-map*

Syntax Description	<i>route-map</i>	Specifies the route map to be used as an export route map for the VRF.
---------------------------	------------------	--

Defaults This command has no default behavior.

Command Modes VRF configuration mode

Command History	Release	Modification
	12.0(5)T	This command was introduced.

Usage Guidelines Use an export route map when an application requires finer control over the routes that are exported out of a VRF than the control that is provided by import and export extended communities configured for the importing and exporting VRFs.

The **export map** command associates a route map with the specified VRF. You can use a route map to filter routes that are eligible for export out of a VRF, based on the route target extended community attributes of the route.

Only one export route map per VRF is supported.

Examples The following example shows how to configure an export route map for a VRF:

```
Router(config)# ip vrf vrf_red
Router(config-vrf)# export map blue_export_map
```

Related Commands	Command	Description
	import map	Configures an import route map for a VRF.
	ip extcommunity-list	Creates an extended community list for BGP and controls access to it.
	ip vrf	Configures a VRF routing table.
	route-target	Creates a route-target extended community for a VRF.
	show ip vrf	Displays the set of defined VRFs and associated interfaces.

ip as-path access-list

To define a BGP autonomous system path access list, use the **ip as-path access-list** command in global configuration mode. 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-regexp*

no ip as-path access-list *access-list-number*

Syntax Description	
<i>access-list-number</i>	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.
<i>as-regexp</i>	Autonomous system in the access list using a regular expression. Refer to the “Regular Expressions” appendix in the <i>Cisco IOS Terminal Services Configuration Guide</i> for information about forming regular expressions.

Defaults No access lists are defined.

Command Modes Global configuration

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines You can specify an access list filter on both inbound and outbound BGP routes. 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.

Examples The following example specifies that the BGP neighbor with IP address 172.16.1.1 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 10.108.0.0
 neighbor 192.168.6.6 remote-as 123
 neighbor 172.16.1.1 remote-as 47
 neighbor 172.16.1.1 filter-list 1 out
```

Related Commands

Command	Description
neighbor distribute-list	Distributes BGP neighbor information as specified in an access list.
neighbor filter-list	Sets up a BGP filter.

ip bgp-community new-format

To display BGP communities in the format AA:NN (autonomous system-community number/2-byte number), use the **ip bgp-community new-format** command in global configuration mode. To reenabte the previous display format for BGP communities (one 32-bit number), use the **no** form of this command.

ip bgp-community new-format

no ip bgp-community new-format

Syntax Description

This command has no argument or keywords.

Defaults

BGP communities are displayed in the Cisco default format, one 32-bit number.

Command Modes

Global configuration

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

RFC 1997, *BGP Communities Attribute* specifies that a BGP community is made up of two parts that are 2 bytes long. The first part is the autonomous system number and the second part is a 2-byte number. In the most recent version of the RFC, a community is of the form AA:NN. The Cisco default community format is one 32-bit number. The **ip bgp-community new-format** command changes the community format to AA:NN to conform to RFC 1997.

Examples

The following example upgrades a router that uses the 32-bit number community format to the AA:NN format:

```
Router(config)# ip bgp-community new-format
```

The following example shows how BGP community numbers are displayed when the **ip bgp-community new-format** command is enabled:

```
Router# show ip bgp 10.0.0.0
```

```
BGP routing table entry for 10.0.0.0/8, version 4
Paths: (2 available, best #2, table Default-IP-Routing-Table)
  Advertised to non peer-group peers:
    10.0.33.35
    35
    10.0.33.35 from 10.0.33.35 (192.168.3.3)
      Origin incomplete, metric 10, localpref 100, valid, external
      Community: 1:1
  Local
    0.0.0.0 from 0.0.0.0 (10.0.33.34)
      Origin incomplete, metric 0, localpref 100, weight 32768, valid, sourced, best
```

Related Commands	Command	Description
	show ip bgp	Displays entries in the BGP routing table.

ip bgp fast-external-fallover

To enable per-interface fast external fallover, enter the **ip bgp fast-external-fallover** command in interface configuration mode. To revert back to the current behavior, use the **no** format of this command.

```
ip bgp fast-external-fallover [permit | deny]
```

```
no ip bgp fast-external-fallover [permit | deny]
```

Syntax Description

permit	Allows per-interface fast external fallover.
deny	Prevents per-interface fast external fallover.

Defaults

Global fast external fallover.

Command Modes

Interface configuration

Command History

Release	Modification
12.0ST	This command was introduced.
12.1	This command was integrated into Cisco IOS Release 12.1.
12.2	This command was integrated into Cisco IOS Release 12.2.

Usage Guidelines

When you specify the **ip bgp fast-external-fallover** command with the **permit** or **deny** keyword, it overrides the global setting. If you enter the **no** format of the command, the global setting is in effect for this interface.

Examples

The following example enables per-interface fast-external-fallover on interface Ethernet 0/0:

```
Router(config)# interface ethernet 0/0  
Router(config-if)# ip bgp fast-external-fallover permit
```

ip community-list

To create or configure a Border Gateway Protocol (BGP) community list and to control access to it, use the **ip community-list command** in global configuration command. To delete the community list, use the **no** form of this command.

```
ip community-list { standard | standard list-name { deny | permit } [community-number] [AA:NN]
  [internet] [local-AS] [no-advertise] [no-export] } | { expanded | expanded list-name { deny |
  permit } regex }
```

```
no ip community-list standard | expanded | { expanded | standard } list-name
```

Syntax Description

<i>standard</i>	Configures a standard community list using a number from 1 to 99 to identify one or more permit or deny groups of communities.
standard <i>list-name</i>	Configures a named standard community list.
permit	Permits access for a matching condition.
deny	Denies access for a matching condition.
<i>community-number</i>	(Optional) Specifies a community as a 32-bit number from 1 to 4294967200. A single community can be entered or multiple communities can be entered, each separated by a space.
<i>AA:NN</i>	(Optional) Autonomous system number and network number entered in the 4-byte new community format. This value is configured with with two 2-byte numbers separated by a colon. A number from 1 to 65535 can be entered each 2-byte number. A single community can be entered or multiple communities can be entered, each separated by a space.
internet	(Optional) Specifies the Internet community. Routes with this community are advertised to all peers (internal and external).
no-export	(Optional) Specifies the no-export community. Routes with this community are advertised to only peers in the same autonomous system or to only other subautonomous systems within a confederation. These routes are not advertised to external peers.
local-as	(Optional) Specifies the local-as community. Routes with community are advertised to only peers that are part of the local autonomous system or to only peers within a subautonomous system of a confederation. These routes are not advertised external peers or to other subautonomous systems within a confederation.
no-advertise	(Optional) Specifies the no-advertise community. Routes with this community are not advertised to any peer (internal or external).
<i>expanded</i>	Configures an expanded community list number from 100 to 500 to identify one or more permit or deny groups of communities.
expanded <i>list-name</i>	Configures a named expanded community list.
<i>regex</i>	Configures a regular expression that is used to specify a pattern to match against an input string.
Note	Regular expressions can be used only with expanded community lists

Defaults

BGP community exchange is not enabled by default. It is enabled on a per-neighbor basis with the **neighbor send-community** command.

The Internet community is applied to all routes or prefixes by default, until any other community value is configured with this command or the **set community** command.

Once a permit value has been configured to match a given set of communities, the community list defaults to an implicit deny for all other community values.

Community values entered in the new format (AA:NN) are converted to 32-bit numbers if the **ip bgp-community new-format** command is not enabled on the local router.

Defaults

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.0	Support for the local-as community was introduced.
12.0(10)S	Named community list support was added.
12.0(16)ST	Named community list support was introduced.
12.1(9)E	Named community list support was integrated into Cisco IOS Release 12.1(9)E.
12.2(8)T	Named community list support was integrated into Cisco IOS Release 12.2(8)T.
12.0(22)S	The maximum number of expanded community list numbers was increased from 199 to 500.
12.2(15)T	The maximum number of expanded community list numbers was increased from 199 to 500.

Usage Guidelines

The **ip community-list** command is used to configure BGP community filtering. BGP community values are configured as a 32-bit number (old format) or as a 4-byte number (new format). The new community format is enabled when the **ip bgp-community new-format** command is entered in global configuration mode. The new community format consists of a 4-byte value. The first two bytes represent the autonomous system number, and the trailing two bytes represent a user-defined network number. Named and numbered community lists are supported. BGP community attribute exchange between BGP peers is enabled when the **neighbor send-community** command is configured for the specified neighbor. The BGP community attribute is defined in *RFC-1997* and *RFC-1998*.

Standard Community Lists

Standard community lists are used to configure well-known communities and specific community numbers. A maximum of 16 communities can be configured in a standard community list. If you attempt to configure more than 16 communities, the trailing communities that exceed the limit are not processed or saved to the running configuration file.

Expanded Community Lists

Expanded community lists are used to filter communities using a regular expression. Regular expressions are used to configure patterns to match community attributes. The order for matching using the * or + character is longest construct first. Nested constructs are matched from the outside in.

Concatenated constructs are matched beginning at the left side. If a regular expression can match two different parts of an input string, it will match the earliest part first. For more information about configuring regular expressions, see the *Regular Expressions* appendix of the *Cisco IOS Terminal Services Configuration Guide*.

Community List Processing

When multiple values are configured in the same community list statement, a logical AND condition is created. All community values must match to satisfy an AND condition. When multiple values are configured in separate community list statements, a logical OR condition is created. The first list that matches a condition is processed.

Examples

In the following example, a standard community list is configured that permits routes that from network 10 in autonomous system 50000:

```
Router(config)# ip community-list 1 permit 50000:10
```

In the following example, a standard community list is configured that permits only routes from peers in the same autonomous system or from subautonomous system peers in the same confederation:

```
Router(config)# ip community-list 1 permit no-export
```

In the following example, a standard community list is configured to deny routes that carry communities from network 40 in autonomous system 65534 and from network 60 in autonomous system 65412. This example shows a logical AND condition; all community values must match in order for the list to be processed.

```
Router(config)# ip community-list 2 deny 65534:40 65412:60
```

In the following example, a named standard community list is configured that permits all routes within the local autonomous system or permits routes from network 20 in autonomous system 40000. This example shows a logical OR condition; the first match is processed.

```
Router(config)# ip community-list standard RED permit local-AS
Router(config)# ip community-list standard RED permit 40000:20
```

In the following example, an expanded community list is configured that will deny routes that carry communities from any private autonomous system:

```
Router(config)# ip community-list 500 deny _64[6-9][0-9][0-9]_|_65[0-9][0-9][0-9]_
```

In the following example, a named expanded community list configured that denies routes from network 1 through 99 in autonomous system 50000:

```
Router(config)# ip community-list expanded BLUE deny 50000:[0-9][0-9]_
```

Related Commands

Command	Description
match community	Matches a BGP community.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set community	Sets the BGP communities attribute.
set comm-list delete	Removes communities from the community attribute of an inbound or outbound update.

Command	Description
show ip bgp community	Displays routes that belong to specified BGP communities.
show ip bgp regexp	Displays routes that match a locally configured regular expression.

ip extcommunity-list

To create an extended community access list and control access to it, use the **ip extcommunity-list** command in global configuration mode. To delete the community list, use the **no** form of this command.

```
ip extcommunity-list standard-list-number expanded-list-number { permit | deny }
    [regular-expression] [rt | soo extended-community-value]
```

```
no ip extcommunity-list
```

Syntax Description

<i>standard-list-number</i>	Integer from 1 to 99 that identifies one or more permit or deny groups of extended communities.
<i>expanded-list-number</i>	Integer from 100 to 500 that identifies one or more permit or deny groups of extended communities. Regular expressions can be configured with expanded lists but not standard lists.
permit	Permits access for a matching condition.
deny	Denies access for a matching condition.
<i>regular-expression</i>	(Optional) An input string pattern to match against.
rt	(Optional) Specifies the route target (RT) extended community attribute. The rt keyword can be configured only with standard extended community lists and not expanded community lists.
soo	(Optional) Specifies the site of origin (SOO) extended community attribute. The soo keyword can be configured only with standard extended community lists and not expanded community lists.
<i>extended-community-value</i>	Specifies the route target or site of origin. The value can be one of the following combinations: <ul style="list-style-type: none"> <i>autonomous-system-number:network-number</i> <i>ip-address:network-number</i> The colon is used to separate the autonomous system number and network number or IP address and network number.

Defaults

Once you permit a value for the community number, the community list defaults to an implicit deny for everything else that has not been permitted.

Command Modes

Global configuration

Command History

Release	Modification
12.1	This command was introduced.

Usage Guidelines

Extended community attributes are used to configure, filter, and identify routes for virtual routing and forwarding instances (VRFs) and Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs).

The **ip extcommunity-list** command is used to configure extended community lists. All of the standard rules of access lists apply to the configuration of extended community lists. Regular expressions are supported by the expanded range of extended community list numbers. All regular expression configuration options are supported.

The route target (RT) extended community attribute is configured with the **rt** keyword. This attribute is used to identify a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that are used for routing traffic that is received from corresponding sites.

The site of origin (SOO) extended community attribute is configured with the **soo** keyword. This attribute uniquely identifies the site from which the provider edge (PE) router learned the route. All routes learned from a particular site must be assigned the same site of origin extended community attribute, regardless if a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents routing loops from occurring when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO can be applied to routes that are learned from VRFs. The SOO should not be configured for stub sites or sites that are not multihomed.

Examples

The following example configures an extended community list that will permit routes from route target 901:10 and site of origin 802:20 and deny routes from route target 703:30 and site of origin 604:40:

```
Router(config)# ip extcommunity-list 1 permit rt 901:10
Router(config)# ip extcommunity-list 1 permit soo 802:20
Router(config)# ip extcommunity-list 1 deny rt 703:30 soo 604:40
```

The following example configures an extended community list (in the expanded range) that specifies that the BGP neighbor with IP address 192.168.1.1 is not sent advertisements about any path through or from autonomous system 123:

```
Router(config)# ip extcommunity-list 500 deny _123_
Router(config)# ip extcommunity-list 500 deny ^123 .*
Router(config)# router bgp 101
Router(config-router)# network 172.16.0.0
Router(config-router)# neighbor 10.140.6.6 remote-as 123
Router(config-router)# neighbor 192.168.1.1 remote-as 47
Router(config-router)# neighbor 10.125.1.1 filter-list 1 out
```

The following example configures an extended community list (in the expanded range) that permits routes from autonomous system 123 and denies all other routes:

```
Router(config)# ip extcommunity-list 500 permit (1-3)*
Router(config)# ip extcommunity-list 500 deny (^0-9)*
```

The following example configures an expanded extended community list that permits advertisements that contain a route target extended community attribute beginning with the pattern 100:.

```
Router(config)# ip extcommunity-list 101 permit RT:100:+
```

**Note**

For information about regular expressions and how to use them, see [Regular Expressions](#).

Related Commands

Command	Description
export map	Configures an export route map for a VRF.
match community	Matches a BGP VPN extended community list.
set extcommunity	Sets BGP extended community attributes.
show ip extcommunity-list	Displays routes that are permitted by the extended community list.
show route-map	Displays configured route maps.

ip prefix-list

To create a prefix list or add a prefix-list entry, use the **ip prefix-list** command in global configuration mode. To delete a prefix-list entry, use the **no** form of this command.

```
ip prefix-list {list-name | list-number} [seq number] {deny network/length | permit
network/length} [ge ge-length] [le le-length]
```

```
no ip prefix-list {list-name | list-number} [seq number] {deny network/length | permit
network/length} [ge ge-length] [le le-length]
```

Syntax Description	
<i>list-name</i>	Configures a name to identify the prefix list.
<i>list-number</i>	Configures a number to identify the prefix list.
seq <i>number</i>	(Optional) Applies a sequence number to a prefix-list entry. The range of sequence numbers that can be entered is from 1 to 4294967294. If a sequence number is not entered when configuring this command, a default sequence numbering is applied to the prefix list. The number 5 is applied to the first prefix entry, and subsequent unnumbered entries are incremented by 5.
deny	Denies access for a matching condition.
permit	Permits access for a matching condition.
<i>network/length</i>	Configures the network address, and the length of the network mask in bits. The network number can be any valid IP address or prefix. The bit mask can be a number from 0 to 32.
ge <i>ge-length</i>	(Optional) Specifies the lesser value of a range (the “from” portion of the range description) by applying the <i>ge-length</i> argument to the range specified. The <i>ge-length</i> argument represents the minimum prefix length to be matched. Note The ge keyword represents the greater than or equal to operator.
le <i>le-length</i>	(Optional) Specifies the greater value of a range (the “to” portion of the range description) by applying the <i>le-length</i> argument to the range specified. The <i>le-length</i> argument represents the maximum prefix length to be matched. Note The le keyword represents the less than or equal to operator.

Defaults No prefix lists are created.

Command Modes Global configuration

Command History	Release	Modification
	12.0(3)T	This command was introduced.

Usage Guidelines

When multiple entries of a prefix list match a given prefix, the longest, most specific match is chosen. The router begins the search at the top of the prefix list, with the sequence number 1. Once a match or deny occurs, the router need not go through the rest of the prefix list. For efficiency, you may want to put the most common matches or denials near the top of the list, using the *seq-number* argument in the **ip prefix-list** command. The **show** commands always include the sequence numbers in their output.

By default, the sequence numbers are automatically generated. They can be suppressed with the **no ip prefix-list seq** command. Sequence values are generated in increments of 5. The first sequence value generated in a prefix list would be 5, then 10, then 15, and so on. If you specify a value for an entry and then do not specify values for subsequent entries, the assigned (generated) sequence values are incremented in units of 5. For example, if you specify that the first entry in the prefix list has a sequence value of 3 and then do not specify sequence values for the other entries, the automatically generated numbers will be 8, 13, 18, and so on.

The **ge** and **le** keywords can be used to specify the range of the prefix length to be matched for prefixes that are more specific than the *network/length* argument. Exact match is assumed when neither **ge** nor **le** is specified. The range is assumed to be from *ge-length* to 32 if only the **ge** attribute is specified. The range is assumed to be from **len** to *le-length* if only the **le** attribute is specified.

A specified *ge-length* and/or *le-value* must satisfy the following condition:

$$length < ge-length < le-length \leq 32$$

Notes:

- If you use the **ip prefix-list** command with the **default-information originate** command to generate default routes, specify only IP address matching. Avoid using the **ge** and **le** keywords.

For example, the following command works:

```
ip prefix-list anyrtcondition seq 5 permit 0.0.0.0/0
```

However, the following command is not supported:

```
ip prefix-list anyrtcondition seq 5 permit 0.0.0.0/0 le 32
```

- Using the **ip prefix-list** command with the **route-map** and **match ip next-hop** commands is not supported. Only IP address match clauses are supported.

Examples

The following examples show how a prefix list can be used.

To deny the default route 0.0.0.0/0:

```
ip prefix-list abc deny 0.0.0.0/0
```

To permit the prefix 10.0.0.0/8:

```
ip prefix-list abc permit 10.0.0.0/8
```

The following examples show how to specify a group of prefixes.

To accept a mask length of up to 24 bits in routes with the prefix 192/16:

```
ip prefix-list abc permit 192.168.0.0/16 le 24
```

To deny mask lengths greater than 25 bits in routes with the prefix 192/16:

```
ip prefix-list abc deny 192.168.0.0/16 ge 25
```

To permit mask lengths from 8 to 24 bits in all address space:

```
ip prefix-list abc permit 0.0.0.0/0 ge 8 le 24
```

To deny mask lengths greater than 25 bits in all address space:

```
ip prefix-list abc deny 0.0.0.0/0 ge 25
```

To deny all mask lengths within the network 10/8:

```
ip prefix-list abc deny 10.0.0.0/8 le 32
```

To deny all masks with a length greater than or equal to 25 bits within the network 192.168.1/24:

```
ip prefix-list abc deny 192.168.1.0/24 ge 25
```

To permit all routes:

```
ip prefix-list abc permit 0.0.0.0/0 le 32
```

Related Commands

Command	Description
clear ip prefix-list	Resets the hit count of the prefix list entries.
ip prefix-list description	Adds a text description of a prefix list.
ip prefix-list sequence-number	Enables the generation of sequence numbers for entries in a prefix list.
match route-type (IP)	Redistributes routes of the specified type.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
neighbor prefix-list	Distributes BGP neighbor information as specified in a prefix list.
show ip prefix-list	Displays information about a prefix list or prefix list entries.

ip prefix-list description

To add a text description of a prefix list, use the **ip prefix-list description** command in global configuration mode. To remove the text description, use the **no** form of this command.

ip prefix-list *list-name* *sequence-number* **description** *text*

no ip prefix-list *list-name* *sequence-number* **description** *text*

Syntax Description

<i>list name</i>	Prefix list name.
<i>sequence-number</i>	Sequence number of the prefix list.
<i>text</i>	Text description of te prefix list.

Defaults

There is no text description.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
11.2	The <i>access-list-name</i> , <i>type</i> , and <i>number</i> arguments were added.
12.0	The <i>prefix-list</i> argument was added.

Usage Guidelines

This command is not supported in the Intermediate System-to-Intermediate System (IS-IS) or Open Shortest Path First (OSPF) protocols.

To suppress networks from being advertised in updates, use the **distribute-list out** command.

Examples

The following example shows a prefix list description that indicates which routes are permitted by the prefix list:

```
ip prefix-list customerA description Permit routes from customer A
```

Related Commands	Command	Description
	clear ip prefix-list	Resets the hit count of the prefix list entries.
	distribute-list out	Suppresses networks from being advertised in updates.
	ip prefix-list	Creates an entry in a prefix list.
	ip prefix-list sequence-number	Enables the generation of sequence numbers for entries in a prefix list.
	match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
	neighbor prefix-list	Distributes BGP neighbor information as specified in a prefix list.
	show ip prefix-list	Displays information about a prefix list or prefix list entries.

ip prefix-list sequence-number

To enable the generation of sequence numbers for entries in a prefix list, use the **ip prefix-list sequence-number** command in global configuration mode. To remove the text description, use the **no** form of this command.

ip prefix-list sequence-number

no ip prefix-list sequence-number

Syntax Description This command has no arguments or keywords.

Defaults There is no text description.

Command Modes Global configuration

Command History

Release	Modification
12.0	This command was introduced.

Examples

The following example disables the default automatic generation of sequence numbers for prefix list entries:

```
no ip prefix-list sequence-number
```

Related Commands

Command	Description
clear ip prefix-list	Resets the hit count of the prefix list entries.
distribute-list in	Filters networks received in updates.
distribute-list out	Suppresses networks from being advertised in updates.
ip prefix-list	Creates an entry in a prefix list.
ip prefix-list sequence-number	Enables the generation of sequence numbers for entries in a prefix list.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
neighbor prefix-list	Distributes BGP neighbor information as specified in a prefix list.
show ip prefix-list	Displays information about a prefix list or prefix list entries.

match as-path

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

match as-path *path-list-number*

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

Syntax Description	<i>path-list-number</i> Autonomous system path access list. An integer from 1 to 199.
---------------------------	---

Defaults	No path lists are defined.
-----------------	----------------------------

Command Modes	Route-map configuration
----------------------	-------------------------

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines

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

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

Examples

The following example sets the autonomous system path to match BGP autonomous system path access list 20:

```
route-map igp2bgp
 match as-path 20
```

Related Commands	Command	Description
	match community	Matches a BGP community.
	match interface (IP)	Distributes routes that have their next hop out one of the interfaces specified.
	match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
	match ip next-hop	Redistributes any routes that have a next hop router address passed by one of the access lists specified.

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

match community

To match a Border Gateway Protocol (BGP) community, use the **match community** command in route-map configuration mode. To remove the **match community** command from the configuration file and restore the system to its default condition where the software removes the BGP community list entry, use the **no** form of this command.

```
match community {standard-list-number | expanded-list-number | community-list-name
[exact-match]}
```

```
no match community {standard-list-number | expanded-list-number | community-list-name
[exact-match]}
```

Syntax Description		
<i>standard-list-number</i>	Specifies a standard community list number from 1 to 99 that identifies one or more permit or deny groups of communities.	
<i>expanded-list-number</i>	Specifies an expanded community list number from 100 to 199 that identifies one or more permit or deny groups of communities.	
<i>community-list-name</i>	The community list name.	
exact-match	(Optional) Indicates that an exact match is required. All of the communities and only those communities specified must be present.	

Defaults No community list is matched by the route map.

Command Modes Route-map configuration

Command History	Release	Modification
	10.3	This command was introduced.

Usage Guidelines A route map can have several parts. Any route that does not match at least one **match** command 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 number or name is one of the types of **match** commands applicable to BGP.

Examples

The following example shows that the routes matching community list 1 will have the weight set to 100. Any route that has community 109 will have the weight set to 100.

```
Router(config)# ip community-list 1 permit 109
Router(config)# !
Router(config)# route-map set_weight
Router(config-route-map)# match community 1
Router(config-route-map)# set weight 100
```

The following example shows that the routes matching community list 1 will have the weight set to 200. Any route that has community 109 alone will have the weight set to 200.

```
Router(config)# ip community-list 1 permit 109
Router(config)# !
Router(config)# route-map set_weight
Router(config-route-map)# match community 1 exact
Router(config-route-map)# set weight 200
```

In the following example, the routes that match community list LIST_NAME will have the weight set to 100. Any route that has community 101 alone will have the weight set to 100.

```
Router(config)# ip community-list 1 permit 101
Router(config)# !
Router(config)# route-map set_weight
Router(config-route-map)# match community LIST_NAME
Router(config-route-map)# set weight 100
```

Related Commands

Command	Description
ip community-list	Creates a community list for BGP and controls access to it.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another.
set weight	Specifies the BGP weight for the routing table.

match extcommunity

To match Border Gateway Protocol (BGP) extended community list attributes, use the **match extcommunity** command in route-map configuration mode. To remove the **match extcommunity** command from the configuration file and remove the BGP extended community list attribute entry, use the **no** form of this command.

match extcommunity *standard-list-number* | *expanded-list-number*

no match extcommunity *standard-list-number* | *extended-list-number*

Syntax Description	
<i>standard-list-number</i>	A standard extended community list number from 1 to 99 that identifies one or more permit or deny groups of extended community attributes.
<i>expanded-list-number</i>	An expanded extended community list number from 100 to 500 that identifies one or more permit or deny groups of extended community attributes.

Defaults This command is disabled by default.

Command Modes Route-map configuration

Command History	Release	Modification
	12.1	This command was introduced.

Usage Guidelines Extended community attributes are used to configure, filter, and identify routes for virtual routing and forwarding instances (VRFs) and Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs).

The **match extcommunity** command is used to configure match clauses that use extended community attributes in route maps. The range of numbers that can be configured with the **match extcommunity** command is from 1 to 99. All of the standard rules of match and set clauses apply to the configuration of extended community attributes.

Examples The following example shows that the routes that match extended community list 1 will have the weight set to 100. Any route that has extended community 1 will have the weight set to 100.

```
Router(config)# ip extcommunity-list 1 rt 100:2
Router(config)# !
Router(config)# route-map MAP_NAME permit 10
Router(config-route-map)# match extcommunity 1
Router(config-route-map)# set weight 100
```

Related Commands

Command	Description
ip extcommunity-list	Creates an extended community list for BGP and controls access to it.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another.
set extcommunity	Sets BGP extended community attributes.
set weight	Specifies the BGP weight for the routing table.
show ip bgp filter-list	Displays routes that are permitted by the extended community list.
show route-map	Displays configured route maps.

maximum-paths

To configure the maximum number of parallel routes that an IP routing protocol will install into the routing table, use the **maximum-paths** command in router configuration or address family configuration mode. To restore the default value, use the **no** form of this command.

maximum-paths *number* [**import** *number*]| **import** *number*

no maximum-paths *number* | **import** *number*

Syntax Description

<i>number</i>	Specifies the number of routes to install to the routing table. See the usage guidelines for the number of paths that can be configured with this argument.
import <i>number</i>	(Optional) Specifies the number of redundant paths that can be configured as back up multipaths for a VRF. This keyword can only be configured under a VRF in address family configuration mode.
Note	We recommend that this feature is enabled only where needed and that the number of import paths be kept to the minimum (Typically, not more than two paths). For more information, see the related note in the usage guidelines of this command reference page.

Defaults

Border Gateway Protocol (BGP) by default will install only one best path in the routing table. The default for all other IP routing protocols is four paths.

Command Modes

Router configuration
Address family configuration

Command History

Release	Modification
11.2	This command was introduced.
12.0(25)S	The import keyword was introduced.
12.2(13)T	The import keyword was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	The import keyword was integrated into Cisco IOS Release 12.2(14)S.

Usage Guidelines

The **maximum-paths** command is used to set the number of parallel (equal-cost) routes that BGP will install in the routing table to configure multipath loadsharing. The number of paths that can be configured is determined by the version of Cisco IOS software. The following list shows current limits:

- Cisco IOS Release 12.0S based software: 8 paths
- Cisco IOS Release 12.3T based software: 16 paths
- Cisco IOS Release 12.2S based software: 32 paths

The **maximum-paths** command cannot be configured with the **maximum-paths eibgp** command for the same BGP routing process.

Configuring VRF Import Paths

A VRF will import only one path (best path) per prefix from the source VRF table, unless the prefix is exported with a different route-target. If the best path goes down, the destination will not be reachable until the next import event occurs, and then a new best path will be imported into the VRF table. The import event runs every 15 seconds by default.

The **import** keyword allows you to configure the VRF table to accept multiple redundant paths in addition to the best path. An import path is a redundant path, and it can have a next hop that matches an installed multipath. This feature should be used when there are multiple paths with identical next hops available to ensure optimal convergence times. A typical application of this feature is to configure redundant paths in a network that has multiple route reflectors for redundancy.



Note

Configuring redundant paths with the **import** keyword can increase CPU and memory utilization significantly, especially in a network where there are many prefixes to learn and a large number of configured VRFs. It is recommended that this feature is only configured as necessary and that the minimum number of redundant paths are configured (Typically, not more than two).

Examples

In the following example, the router is configured to install 2 parallel routes in the BGP routing table:

```
Router(config)# router bgp 40000  
Router(config-router)# maximum-paths 2
```

In the following example, the router is configured to install 6 equal-cost routes and 2 import routes (backup) in the VRF routing table:

```
Router(config)# router bgp 40000  
Router(config-router)# address-family ipv4 vrf RED  
Router(config-router-af)# maximum-paths 6 import 2
```

In the following example, the router is configured to install 2 import routes in the VRF routing table:

```
Router(config)# router bgp 100  
Router(config-router)# address-family ipv4 vrf BLUE  
Router(config-router-af)# maximum-paths import 2
```

neighbor advertisement-interval

To set the minimum interval between the sending of BGP routing updates, use the **neighbor advertisement-interval** command in address family or router configuration mode. 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>	IP address of the number.
<i>peer-group-name</i>	Name of a BGP peer group.
<i>seconds</i>	Time (in seconds) is specified by an integer from 0 to 600.

Defaults

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

Command Modes

Address family configuration
Router configuration

Command History

Release	Modification
10.3	This command was introduced.
12.0(7)T	Address family configuration mode was added.

Usage Guidelines

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

Examples

The following router configuration mode example sets the minimum time between sending BGP routing updates to 10 seconds:

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

The following address family configuration mode example sets the minimum time between sending BGP routing updates to 10 seconds:

```
router bgp 5
 address-family ipv4 unicast
 neighbor 4.4.4.4 advertisement-interval 10
```

Related Commands	Command	Description
	address-family ipv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
	address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
	neighbor peer-group (creating)	Creates a BGP peer group.

neighbor advertise-map

To install a Border Gateway Protocol (BGP) route as a locally originated route in the BGP routing table for conditional advertisement, use the **neighbor advertise-map** command in router configuration mode. To disable conditional advertisement, use the **no** form of this command.

```
neighbor ip-address advertise-map map-name {non-exist-map map-name}
```

```
no neighbor ip-address advertise-map map-name {non-exist-map map-name}
```

Syntax Description

<i>ip-address</i>	Specifies the IP address of the router that should receive conditional advertisements.
advertise-map <i>map-name</i>	Specifies the name of the route map that will be advertised if the conditions of the exist map or nonexist map are met.
non-exist-map <i>map-name</i>	Specifies the name of the route map that will be compared to the advertise map. If the condition is met and no match occurs, the route will be advertised. If a match occurs, then the condition is not met, and the route is withdrawn.

Defaults

No default behavior or values

Command Modes

Address family
Router configuration

Command History

Release	Modification
11.1CC	This command was introduced.
11.2	This command was integrated into Cisco IOS Release 11.2.

Usage Guidelines

Use the **neighbor advertise-map** router configuration command to conditionally advertise selected routes. The routes or prefixes that will be conditionally advertised are defined in 2 route-maps, an advertise map and a nonexist map. The route map associated with the nonexist map specifies the prefix that the BGP speaker will track. The route map associated with the advertise-map specifies the prefix that will be advertised to the specified neighbor when the condition is met. When configuring a nonexist map, the condition is met when the prefix exists in the advertise map but does not exist in the nonexist map. If the condition is not met, the route is withdrawn and conditional advertisement does not occur. All routes that may be dynamically advertised or not advertised need to exist in the BGP routing table for conditional advertisement to occur.

Examples

The following address family configuration example configures BGP to conditionally advertise a prefix to the 10.1.1.1 neighbor using a nonexistent map. If the prefix exists in MAP3 but not MAP4, the condition is met and the prefix is advertised.

```
router bgp 5
 address-family ipv4 multicast
 neighbor 10.1.1.1 advertise-map MAP3 non-exist-map MAP4
```

Related Commands

Command	Description
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
route-map	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.

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** command in address family or router configuration mode. To send no route as a default, 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>	IP address of the neighbor.
<i>peer-group-name</i>	Name of a BGP peer group.
route-map <i>map-name</i>	(Optional) Name of the route map. The route map allows route 0.0.0.0 to be injected conditionally.

Defaults

No default route is sent to the neighbor.

Command Modes

Address family configuration
Router configuration

Command History

Release	Modification
11.0	This command was introduced.
12.0	Modifications were added to permit extended access lists.
12.0(7)T	Address family configuration mode was added.

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.

You can use standard or extended access lists with the **neighbor default-originate** command.

Examples

In the following router configuration example, the local router injects route 0.0.0.0 to the neighbor 172.16.2.3 unconditionally:

```
router bgp 109
 network 172.16.0.0
 neighbor 172.16.2.3 remote-as 200
 neighbor 172.16.2.3 default-originate
```

In the following address family configuration example, the local router injects route 0.0.0.0 to the neighbor 172.16.2.3 unconditionally:

```
router bgp 109
neighbor 172.16.2.3 remote-as 200
address-family ipv4 unicast
network 172.16.0.0
neighbor 172.16.2.3 default-originate
```

In the following example, the local router injects route 0.0.0.0 to the neighbor 172.16.2.3 only if there is a route to 198.92.68.0 (that is, if a route with any mask exists, such as 255.255.255.0 or 255.255.0.0):

```
router bgp 109
network 172.16.0.0
neighbor 172.16.2.3 remote-as 200
neighbor 172.16.2.3 default-originate route-map default-map
!
route-map default-map 10 permit
match ip address 1
!
access-list 1 permit 198.92.68.0
```

In the following example, the last line of the configuration has been changed to show the use of an extended access list. The local router injects route 0.0.0.0 to the neighbor 172.16.2.3 only if there is a route to 198.92.68.0 with a mask of 255.255.0.0:

```
router bgp 109
network 172.16.0.0
neighbor 172.16.2.3 remote-as 200
neighbor 172.16.2.3 default-originate route-map default-map
!
route-map default-map 10 permit
match ip address 1
!
access-list 100 permit ip host 198.92.68.0 host 255.255.255.0
```

Related Commands

Command	Description
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
neighbor ebgp-multihop	Accepts and attempts BGP connections to external peers residing on networks that are not directly connected.

neighbor description

To associate a description with a neighbor, use the **neighbor description** command in router configuration mode. To remove the description, use the **no** form of this command.

```
neighbor {ip-address | peer-group-name} description text
```

```
no neighbor {ip-address | peer-group-name} description [text]
```

Syntax Description

<i>ip-address</i>	IP address of the neighbor.
<i>peer-group-name</i>	Name of a BGP peer group.
<i>text</i>	Text (up to 80 characters) that describes the neighbor.

Defaults

There is no description of the neighbor.

Command Modes

Router configuration

Command History

Release	Modification
11.3	This command was introduced.

Examples

In the following example, the description of the neighbor is “peer with xyz.com”:

```
router bgp 109
 network 172.16.0.0
 neighbor 172.16.2.3 description peer with xyz.com
```

neighbor distribute-list

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

neighbor {*ip-address* | *peer-group-name*} **distribute-list** {*access-list-number* | *expanded-list-number* | *access-list-name* | *prefix-list-name*} {**in** | **out**}

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

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 a standard or extended access list. The range of a standard access list number is from 1 to 99. The range of an extended access list number is from 100 to 199.
<i>expanded-list-number</i>	Number of an expanded access list number. The range of an expanded access list is from 1300 to 2699.
<i>access-list-name</i>	Name of a standard or extended access list.
<i>prefix-list-name</i>	Name of a BGP prefix list.
in	Access list is applied to incoming advertisements to that neighbor.
out	Access list is applied to outgoing advertisements to that neighbor.

Defaults

No BGP neighbor is specified.

Command Modes

Address family configuration
Router configuration

Command History

Release	Modification
10.0	This command was introduced.
11.0	The <i>peer-group-name</i> argument was added.
11.2	The <i>access-list-name</i> argument was added.
12.0	The <i>prefix-list-name</i> argument was added.
12.0(7)T	Address family configuration mode was added.

Usage Guidelines

If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command. Specifying the command for a neighbor overrides the inbound policy that is inherited from the peer group.

Using a distribute list is one of several ways to filter advertisements. Advertisements can also be filtered by using the following methods:

- Autonomous system path filters can be configured with the **ip as-path access-list** and **neighbor filter-list** commands.
- The **access-list (IP standard)** and **access-list (IP extended)** commands can be used to configure standard and extended access lists for the filtering of advertisement.
- The **route map** command can be used to filter advertisements. Route maps may be configured with autonomous system filters, prefix filters, access lists and distribute lists.

Standard access lists may be used to filter routing updates. However, in the case of route filtering when using classless interdomain routing (CIDR), standard access lists do not provide the level of granularity that is necessary to configure advanced filtering of network addresses and masks. Extended access lists, configured with the **access-list (IP extended)** command, should be used to configure route filtering when using CIDR because extended access lists allow the network operator to use wild card bits to filter the relevant prefixes and masks. Wild card bits are similar to the bit masks that are used with normal access lists; prefix and mask bits that correspond to wild card bits that are set to 0 are used in the comparison of addresses or prefixes and wild card bits that are set to 1 are ignored during any comparisons. This function of extended access list configuration can also be used to filter addresses or prefixes based on the prefix length.

**Note**

Do not apply both a **neighbor distribute-list** and a **neighbor prefix-list** command to a neighbor in any given direction (inbound or outbound). These two commands are mutually exclusive, and only one command (**neighbor prefix-list** or **neighbor distribute-list**) can be applied to each inbound or outbound direction.

Examples

The following router configuration mode example applies list 39 to incoming advertisements from neighbor 120.23.4.1. List 39 permits the advertisement of network 10.109.0.0.

```
router bgp 109
 network 10.108.0.0
 neighbor 120.23.4.1 distribute-list 39 in
```

The following three examples show different scenarios for using an extended access list with a distribute list. The three examples are labeled “Example A”, “Example B”, and “Example C.” Each of the example extended access list configurations are used with the **neighbor distribute-list** command configuration example below.

```
router bgp 109
 network 10.108.0.0
 neighbor 120.23.4.1 distribute-list 101 in
```

Example A

The following extended access list example will permit route 192.168.0.0 255.255.0.0 but deny any more specific routes of 192.168.0.0 (including 192.168.0.0 255.255.255.0):

```
access-list 101 permit ip 192.168.0.0 0.0.0.0 255.255.0.0 0.0.0.0
access-list 101 deny ip 192.168.0.0 0.0.255.255 255.255.0.0 0.0.255.255
```

Example B

The following extended access list example will permit route 10.108.0/24 but deny 131.108/16 and all other subnets of 10.108.0.0:

```
access-list 101 permit ip 10.108.0.0 0.0.0.0 255.255.255.0 0.0.0.0
access-list 101 deny ip 10.108.0.0 0.0.255.255 255.255.0.0 0.0.255.255
```

Example C

The following extended access list example will deny all prefixes that are longer than 24 bits and permit all of the shorter prefixes:

```
access-list 101 deny ip 0.0.0.0 255.255.255.255 255.255.255.0 0.0.0.255
access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
access-list (IP standard)	Defines a standard IP access list.
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
ip as-path access-list	Defines a BGP-related access list.
neighbor filter-list	Sets up a BGP filter.
neighbor peer-group (creating)	Creates a BGP peer group.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another.

neighbor ebgp-multihop

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

```
neighbor {ip-address | peer-group-name} ebgp-multihop [ttl]
```

```
no neighbor {ip-address | peer-group-name} ebgp-multihop
```

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>	(Optional) Time-to-live in the range from 1 to 255 hops.

Defaults

Only directly connected neighbors are allowed.

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
11.0	The <i>peer-group-name</i> argument was added.

Usage Guidelines

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

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

To prevent the creation of loops through oscillating routes, the multihop will not be established if the only route to the multihop peer is the default route (0.0.0.0).

Examples

The following example allows connections to or from neighbor 10.108.1.1, which resides on a network that is not directly connected:

```
router bgp 109
 neighbor 10.108.1.1 ebgp-multihop
```

Related Commands

Command	Description
neighbor advertise-map non-exist-map	Allows a BGP speaker (the local router) to send the default route 0.0.0.0 to a neighbor for use as a default route.
neighbor peer-group (creating)	Creates a BGP peer group.
network (BGP and multiprotocol BGP)	Specifies the list of networks for the BGP routing process.

neighbor filter-list

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

```
neighbor {ip-address | peer-group-name} filter-list access-list-number {in | out}
```

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

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 applied to incoming routes.
out	Access list applied to outgoing routes.

Defaults

No filter is used.

Command Modes

Address family configuration

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(7)T	Address family configuration mode was added.
12.1	The weight keyword was removed.

Usage Guidelines

This command establishes filters on both inbound and outbound BGP routes.

The weights assigned with the **match as-path** and **set weight** route-map configuration commands override the weights assigned using the **neighbor weight** command.

Refer to the “Regular Expressions” appendix in the *Cisco IOS Terminal Services Configuration Guide* for information on forming regular expressions.

If you specify a BGP peer group by using the *peer-group-name* argument, all 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.

Examples

In the following router configuration mode example, the BGP neighbor with IP address 172.16.1.1 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 10.108.0.0
 neighbor 192.168.6.6 remote-as 123
 neighbor 172.16.1.1 remote-as 47
 neighbor 172.16.1.1 filter-list 1 out
```

In the following address family configuration mode example, the BGP neighbor with IP address 172.16.1.1 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
 address-family ipv4 unicast
 network 10.108.0.0
 neighbor 192.168.6.6 remote-as 123
 neighbor 172.16.1.1 remote-as 47
 neighbor 172.16.1.1 filter-list 1 out
```

Related Commands

Command	Description
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
ip as-path access-list	Defines a BGP-related access list.
match as-path	Match BGP autonomous system path access lists.
neighbor distribute-list	Distributes BGP neighbor information as specified in an access list.
neighbor peer-group (creating)	Creates a BGP peer group.
neighbor weight	Assigns a weight to a neighbor connection.
set weight	Specifies the BGP weight for the routing table

neighbor local-as

To allow customization of the autonomous system number for external Border Gateway Protocol (eBGP) peer groupings, use the **neighbor local-as** command in address family or router configuration mode. To disable this function, use the **no** form of this command.

neighbor {*ip-address* | *peer-group-name*} **local-as** *as-number*

no neighbor {*ip-address* | *peer-group-name*} **local-as** *as-number*

Syntax Description

<i>ip-address</i>	IP address of the local BGP-speaking neighbor.
<i>peer-group-name</i>	Name of a BGP peer group.
<i>as-number</i>	Valid autonomous system number from 1 to 65535. Do not specify the autonomous system number to which the neighbor belongs.

Defaults

This command is disabled by default.

Command Modes

Address family configuration
Router configuration

Command History

Release	Modification
12.0(4.4)S	This command was introduced.
12.0(5)T	Address family configuration mode was added.

Usage Guidelines

Each BGP peer or peer group can be made to have a local autonomous system value for the purpose of peering. In the case of peer groups, the local autonomous system value is valid for all peers in the peer group.

This feature cannot be customized for individual peers in a peer group.

If this command is configured, you cannot use the local BGP autonomous system number or the autonomous system number of the remote peer.

This command is valid only if the peer is a true eBGP peer. This feature does not work for two peers in different subautonomous systems in a confederation.

Examples

The following address family configuration example shows the customization of neighbor 172.20.1.1 configured to have an autonomous system number of 300 for the purpose of peering:

```
router bgp 109
address-family ipv4 multicast
network 172.20.0.0
neighbor 172.20.1.1 local-as 300
```

The following router configuration example shows the customization of neighbor 172.20.1.1 configured to have autonomous system number of 300 for the purpose of peering:

```
router bgp 109
network 172.20.0.0
neighbor 172.20.1.1 local-as 300
```

Related Commands

Command	Description
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
show ip bgp neighbors	Displays information about BGP neighbors.
show ip bgp peer-group	Displays information about BGP peer groups.

neighbor maximum-prefix

To control how many prefixes can be received from a neighbor, use the **neighbor maximum-prefix** command in router configuration mode. To disable this function, use the **no** form of this command.

```
neighbor {ip-address | peer-group-name} maximum-prefix maximum [threshold]
[warning-only]
```

```
no neighbor {ip-address | peer-group-name} maximum-prefix maximum
```

Syntax Description

<i>ip-address</i>	IP address of the neighbor.
<i>peer-group-name</i>	Name of a BGP peer group.
<i>maximum</i>	Maximum number of prefixes allowed from this neighbor.
<i>threshold</i>	(Optional) Integer specifying at what percentage of <i>maximum</i> the router starts to generate a warning message. The range is from 1 to 100; the default is 75 (percent).
warning-only	(Optional) Allows the router to generate a log message when the <i>maximum</i> is exceeded, instead of terminating the peering.

Defaults

This command is disabled by default. There is no limit on the number of prefixes.

Command Modes

Router configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

This command allows you to configure a maximum number of prefixes that a BGP router is allowed to receive from a peer. It adds another mechanism (in addition to distribute lists, filter lists, and route maps) to control prefixes received from a peer.

When the number of received prefixes exceeds the maximum number configured, the router terminates the peering (by default). However, if the **warning-only** keyword is configured, the router instead only sends a log message, but continues peering with the sender. If the peer is terminated, the peer stays down until the **clear ip bgp** command is issued.

Examples

The following example sets the maximum number of prefixes allowed from the neighbor at 192.168.6.6 to 1000:

```
router bgp 109
 network 10.108.0.0
 neighbor 192.168.6.6 maximum-prefix 1000
```

Related Commands

Command	Description
clear ip bgp	Resets a BGP connection using BGP soft reconfiguration.

neighbor next-hop-self

To configure the router as the next hop for a BGP-speaking neighbor or peer group, use the **neighbor next-hop-self** command in router configuration mode. 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

<i>ip-address</i>	IP address of the BGP-speaking neighbor.
<i>peer-group-name</i>	Name of a BGP peer group.

Defaults

This command is disabled by default.

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
11.0	The <i>peer-group-name</i> argument was added.

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 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.

For a finer granularity of control, see the **set ip next-hop** command.

Examples

The following example forces all updates destined for 10.108.1.1 to advertise this router as the next hop:

```
router bgp 109
 neighbor 10.108.1.1 next-hop-self
```

Related Commands

Command	Description
neighbor peer-group (creating)	Creates a BGP peer group.
set ip next-hop (BGP)	Indicates where to output packets that pass a match clause of a route map for policy routing.

neighbor next-hop-unchanged

To enable an external BGP (eBGP) multihop peer to propagate the next hop unchanged, use the **neighbor next-hop-unchanged** command in address family or router configuration mode. To disable next hop propagation capabilities, use the **no** form of this command.

neighbor *ip-address* | *peer-group-name* **next-hop-unchanged**

no neighbor *ip-address* | *peer-group-name* **next-hop-unchanged**

Syntax Description

<i>ip-address</i>	The IP address of the next hop.
<i>peer-group-name</i>	The name of a BGP peer group that is the next hop.

Defaults

No default behavior or values

Command Modes

Address family configuration
Router configuration

Command History

Release	Modification
12.0(16)ST	This command was introduced.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.

Usage Guidelines

The **neighbor next-hop-unchanged** command is used to configured the propagate the next hop unchanged for multihop eBGP peering sessions. The **neighbor next-hop-self** command should not be used to modify the next hop attribute for a route reflector when this feature is enabled for a route reflector client.

This command can be used to perform the following tasks:

- Bring the route reflector into the forwarding path, which can be used with the iBGP Multipath Load Sharing feature to configure load balancing.
- Configure interprovider Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) by not modifying the next hop attribute when advertising routes to an eBGP peer.
- Turn off the next hop calculation for an eBGP peer. This feature is useful for configuring the end-to-end connection of a label-switched path.



Caution

Incorrectly setting BGP attributes for a route reflector can cause inconsistent routing, routing loops, or a loss of connectivity. Setting BGP attributes for a route reflector should be attempted only by an experienced network operator.

Examples**Route Reflector Configuration**

In the following example, the local router is configured as a route reflector and configures the 10.0.0.100 multihop peer as a route reflector client. A route map is created to set the advertised next hop to 172.16.0.1.

```
Router(config)# route-map NEXTHOP
Router(config-route-map)# set ip next-hop 172.16.0.1
Router(config-route-map)# exit
Router(config)# router bgp 65534
Router(config-router)# neighbor 10.0.0.100 remote-as 65412
Router(config-router)# address-family ipv4
Router(config-router-af)# neighbor 10.0.0.100 activate
Router(config-router-af)# neighbor 10.0.0.100 ebgp-multihop 255
Router(config-router-af)# neighbor 10.0.0.100 route-reflector-client
Router(config-router-af)# neighbor 10.0.0.100 route-map NEXTHOP out
Router(config-router-af)# end
```

Route Reflector Client Configuration

In the following example, the local router (route-reflector client) is configured to establish peering with the route reflector and to propagate the next hop unchanged:

```
Router(config)# router bgp 65412
Router(config-router)# neighbor 192.168.0.1 remote-as 65412
Router(config-router)# address-family ipv4
Router(config-router-af)# neighbor 192.168.0.1 activate
Router(config-router-af)# neighbor 192.168.0.1 ebgp-multihop 255
Router(config-router-af)# neighbor 192.168.0.1 next-hop-unchanged
Router(config-router-af)# end
```

Related Commands

Command	Description
address-family ipv4	Enters address family configuration mode for configuring routing sessions, such as BGP, RIP, or static routing sessions, that use standard IPv4 address prefixes.
address-family vpnv4	Enters address family configuration mode for configuring routing sessions, such as BGP, RIP, or static routing sessions, that use standard VPNv4 address prefixes.
neighbor ebgp-multihop	Accepts and attempts BGP connections to external peers residing on networks that are not directly connected.
neighbor route-map	Applies a route map to incoming or outgoing routes.
neighbor route-reflector-client	Configures the router as a BGP route reflector and configures the specified neighbor as its client.

neighbor password

To enable Message Digest 5 (MD5) authentication on a TCP connection between two BGP peers, use the **neighbor password** command in router configuration mode. To disable this function, 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

<i>ip-address</i>	IP address of the BGP-speaking neighbor.
<i>peer-group-name</i>	Name of a BGP peer group.
<i>string</i>	Case-sensitive password of up to 25 characters when the service password-encryption command is enabled and up to 81 characters when the service password-encryption command is not enabled. The first character cannot be a number. The string can contain any alphanumeric characters, including spaces. You cannot specify a password in the format <i>number-space-anything</i> . The space after the number can cause authentication to fail.

Defaults

This command is disabled by default.

Command Modes

Router configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

You can configure MD5 authentication between two BGP peers, meaning that each segment sent on the TCP connection between the peers is verified. MD5 authentication must be configured with the same password on both BGP peers; otherwise, the connection between them will not be made. Configuring MD5 authentication causes the Cisco IOS software to generate and check the MD5 digest of every segment sent on the TCP connection.

When configuring MD5 authentication, you can enter a case-sensitive password of up to 25 characters when the **service password-encryption** command is enabled and up to 81 characters when the **service password-encryption** command is not enabled. The string can contain any alphanumeric characters, including spaces. A password cannot be configured in the number-space-anything format. The space after the number can cause authentication to fail. You can also use any combination of the following symbolic characters along with alphanumeric characters:

```
` ~ ! @ # $ % ^ & * ( ) - _ = + | \ } [ { [ " ' : ; / > < . , ?
```

**Caution**

If the authentication string is configured incorrectly, the BGP peering session will not be established. We recommend that you enter the authentication string carefully and verify that the peering session is established after authentication is configured.

If you specify a BGP peer group by using the *peer-group-name* argument, all 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 such as 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 such as the following will appear on the screen:

```
%TCP-6-BADAUTH: Invalid MD5 digest from [peer's IP address]:11004 to [local router's
IP address]:179
```

Configuring an MD5 Password in an Established BGP Session

If you configure or change the password or key used for MD5 authentication between two BGP peers, the local router will not tear down the existing session after you configure the password. The local router will attempt to maintain the peering session using the new password until the BGP holddown timer expires. The default time period is 180 seconds. If the password is not entered or changed on the remote router before the holddown timer expires, the session will time out.

**Note**

Configuring a new timer value for the holddown timer will only take effect after the session has been reset. So, it is not possible to change the configuration of the holddown timer to avoid resetting the BGP session.

Examples

The following example configures MD5 authentication for the peering session with the 10.108.1.1 neighbor. *The same password must be configured on the remote peer before the holddown timer expires.*

```
router bgp 109
 neighbor 10.108.1.1 password bla4u00=2nkq
```

Related Commands

Command	Description
neighbor peer-group (creating)	Creates a BGP peer group.
service password-encryption	Encrypts passwords.

neighbor peer-group (assigning members)

To configure a BGP neighbor to be a member of a peer group, use the **neighbor peer-group** command in address family or router configuration mode. 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

<i>ip-address</i>	IP address of the BGP neighbor that belongs to the peer group specified by the <i>peer-group-name</i> argument.
<i>peer-group-name</i>	Name of the BGP peer group to which this neighbor belongs.

Defaults

There are no BGP neighbors in a peer group.

Command Modes

Address family configuration
Router configuration

Command History

Release	Modification
11.0	This command was introduced.
12.0(7)T	Address family configuration mode was added.

Usage Guidelines

The neighbor at the IP address indicated inherits all the configured options of the peer group.

Examples

The following router configuration mode example assigns three neighbors to the peer group named internal:

```
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 172.16.232.53 peer-group internal
 neighbor 172.16.232.54 peer-group internal
 neighbor 172.16.232.55 peer-group internal
 neighbor 172.16.232.55 filter-list 3 in
```

The following address family configuration mode example assigns three neighbors to the peer group named internal:

```
router bgp 100
address-family ipv4 unicast
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 172.16.232.53 peer-group internal
neighbor 172.16.232.54 peer-group internal
neighbor 172.16.232.55 peer-group internal
neighbor 172.16.232.55 filter-list 3 in
```

Related Commands

Command	Description
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
neighbor peer-group (creating)	Creates a BGP peer group.
neighbor shutdown	Disables a neighbor or peer group.