

## neighbor (EIGRP)

To define a neighboring router with which to exchange routing information on a router that is running Enhanced Interior Gateway Routing Protocol (EIGRP), use the **neighbor** command in router configuration mode. To remove an entry, use the **no** form of this command.

**neighbor** *ip-address interface-type interface-number*

**no neighbor** *ip-address interface-type interface-number*

Syntax Description		
	<i>ip-address</i>	IP address of a peer router with which routing information will be exchanged.
	<i>interface-type</i>	Interface through which peering is established.
	<i>interface-number</i>	Number of the interface or subinterface.

**Command Default** No neighboring routers are defined.

**Command Modes** Router configuration

Command History	Release	Modification
	10.0	This command was introduced.

**Usage Guidelines** Multiple neighbor statements can be used to establish peering sessions with specific EIGRP neighbors. The interface through which EIGRP will exchange routing updates must be specified in the neighbor statement. The interfaces through which two EIGRP neighbors exchange routing updates must be configured with IP addresses from the same network.



**Note**

Configuring the **passive-interface** command suppresses all incoming and outgoing routing updates and hello messages. EIGRP neighbor adjacencies cannot be established or maintained over an interface that is configured as passive.

**Examples** The following example configures EIGRP peering sessions with the 192.168.1.1 and 192.168.2.2 neighbors:

```
router eigrp 1
 network 192.168.0.0
 neighbor 192.168.1.1 Ethernet 0/0
 neighbor 192.168.2.2 Ethernet 1/1
```

Related Commands	Command	Description
	<b>passive-interface</b>	Disables sending routing updates on an interface.

## neighbor (OSPF)

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

**neighbor** *ip-address* [**priority number**] [**poll-interval seconds**] [**cost number**] [**database-filter all**]

**no neighbor** *ip-address* [**priority number**] [**poll-interval seconds**] [**cost number**] [**database-filter all**]

### Syntax Description

<i>ip-address</i>	Interface IP address of the neighbor.
<b>priority number</b>	(Optional) A number that indicates the router priority value of the nonbroadcast neighbor associated with the IP address specified. The default is 0. This keyword does not apply to point-to-multipoint interfaces.
<b>poll-interval seconds</b>	(Optional) A number value that represents the poll interval time (in seconds). RFC 1247 recommends that this value be much larger than the hello interval. The default is 120 seconds (2 minutes). This keyword does not apply to point-to-multipoint interfaces. The range is from 0 to 4294967295 seconds.
<b>cost number</b>	(Optional) Assigns a cost to the neighbor, in the form of an integer from 1 to 65535. Neighbors with no specific cost configured will assume the cost of the interface, based on the <b>ip ospf cost</b> command. For point-to-multipoint interfaces, the cost keyword and the <i>number</i> argument are the only options that are applicable. This keyword does not apply to nonbroadcast multiaccess (NBMA) networks.
<b>database-filter all</b>	(Optional) Filters outgoing link-state advertisements (LSAs) to an OSPF neighbor.

### Defaults

No configuration is specified.

### Command Modes

Router configuration

### Command History

Release	Modification
10.0	This command was introduced.
11.3 AA	The <b>cost</b> keyword was added.

### Usage Guidelines

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

One neighbor entry must be included in the Cisco IOS software configuration for each known nonbroadcast network neighbor. The neighbor address must be on the primary address of the interface.

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

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

**Note**

You cannot use the **neighbor (OSPF)** command to specify an Open Shortest Path First (OSPF) neighbor on non-broadcast networks within an OSPF Virtual Private Network (VPN) routing instance.

Prior to Cisco IOS Release 12.0, the **neighbor** command applied to NBMA networks only. With Release 12.0, the **neighbor** command applies to NBMA networks and point-to-multipoint networks. On NBMA networks, the **cost** keyword is not accepted.

**Examples**

The following example declares a router at address 192.168.3.4 on a nonbroadcast network, with a priority of 1 and a poll interval of 180 seconds:

```
router ospf 1
  neighbor 192.168.3.4 priority 1 poll-interval 180
```

The following example illustrates a point-to-multipoint network with nonbroadcast:

```
interface Serial0
ip address 10.0.1.1 255.255.255.0
ip ospf network point-to-multipoint non-broadcast
encapsulation frame-relay
no keepalive
frame-relay local-dlci 200
frame-relay map ip 10.0.1.3 202
frame-relay map ip 10.0.1.4 203
frame-relay map ip 10.0.1.5 204
no shut
!
router ospf 1
network 10.0.1.0 0.0.0.255 area 0
neighbor 10.0.1.3 cost 5
neighbor 10.0.1.4 cost 10
neighbor 10.0.1.5 cost 15
```

**Related Commands**

Command	Description
<b>ip ospf priority</b>	Sets the router priority, which helps determine the designated router for this network.

# neighbor (RIP)

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

**neighbor** *ip-address*

**no neighbor** *ip-address*

<b>Syntax Description</b>	<i>ip-address</i> IP address of a peer router with which routing information will be exchanged.
---------------------------	---

<b>Defaults</b>	No neighboring routers are defined.
-----------------	-------------------------------------

<b>Command Modes</b>	Router configuration
----------------------	----------------------

<b>Command History</b>	Release	Modification
	10.0	This command was introduced.

**Usage Guidelines** This command permits the point-to-point (nonbroadcast) exchange of routing information. When it is used in combination with the **passive-interface** router configuration command, routing information can be exchanged between a subset of routers and access servers on a LAN.

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

**Examples** In the following example, RIP updates are sent to all interfaces on network 10.108.0.0 except Ethernet interface 1. However, in this case a **neighbor** router configuration command is included. This command permits the sending of routing updates to specific neighbors. One copy of the routing update is generated per neighbor.

```
router rip
 network 10.108.0.0
 passive-interface ethernet 1
 neighbor 10.108.20.4
```

<b>Related Commands</b>	Command	Description
	<b>passive-interface</b>	Disables sending routing updates on an interface.

## 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 {exist-map map-name | non-exist-map
map-name }
```

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

Syntax Description		
	ip-address	Specifies the IP address of the router that should receive conditional advertisements.
	<b>advertise-map</b> map-name	Specifies the name of the route map that will be advertised if the conditions of the exist map or nonexist map are met.
	<b>exist-map</b> map-name	Specifies the name of the route map that will be compared to the advertise map. If the condition is met and a match occurs between the advertise map and exist map, the route will be advertised. If no match occurs, then the condition is not met, and the route is withdrawn.
	<b>non-exist-map</b> map-name	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 an exist map or nonexist map. The route map associated with the exist map or 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 an exist map, the condition is met when the prefix exists in both the advertise map and the exist map. When configuring a nonexist map, the condition is met when the prefix exists in the advertise map but does not

exist in the nonexistent 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 router configuration example configures BGP to conditionally advertise a prefix to the 10.2.1.1 neighbor using an exist map. If the prefix exists in MAP1 and MAP2, the condition is met and the prefix is advertised.

```
router bgp 50000
 neighbor 10.2.1.1 advertise-map MAP1 exist-map MAP2
```

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 50000
 address-family ipv4 multicast
 neighbor 10.1.1.1 advertise-map MAP3 non-exist-map MAP4
```

### Related Commands

Command	Description
<b>address-family ipv4</b>	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.
<b>address-family vpnv4</b>	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.
<b>route-map</b>	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.

# 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 ranging from 0 to 600.

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

**Command Modes** Address family  
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 50000
 neighbor 10.4.4.4 advertisement-interval 10
```

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

```
router bgp 50000
 address-family ipv4 unicast
 neighbor 10.4.4.4 advertisement-interval 10
```

Related Commands	Command	Description
	<b>address-family ipv4 (BGP)</b>	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.
	<b>address-family vpnv4</b>	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.
	<b>neighbor peer-group (creating)</b>	Creates a BGP peer group.

# neighbor database-filter

To filter outgoing link-state advertisements (LSAs) to an OSPF neighbor, use the **neighbor database-filter** command in router configuration mode. To restore the forwarding of LSAs to the neighbor, use the **no** form of this command.

**neighbor** *ip-address* **database-filter all out** [*cost metric*]

**no neighbor** *ip-address* **database-filter all out**

Syntax Description		
	<i>ip-address</i>	IP address of the neighbor to which outgoing LSAs are blocked.
	<i>cost metric</i>	(Optional) Cost metric configured for the specified neighbor. The range of this value is from 0 to 65535.

**Defaults** This command is disabled by default. All outgoing LSAs are flooded to the neighbor.

**Command Modes** Router configuration

Command History	Release	Modification
	12.0	This command was introduced.

**Usage Guidelines** This command performs the same function that the **ip ospf database-filter** command performs on an interface basis.

**Examples** The following example prevents flooding of OSPF LSAs to point-to-multipoint networks to the neighbor at IP address 10.2.3.4:

```
router ospf 1
 neighbor 10.2.3.4 database-filter all out
```

Related Commands	Command	Description
	<b>ip ospf database-filter all out</b>	Filters outgoing LSAs to an OSPF interface.

# 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.
<b>route-map</b> <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  
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 50000
 network 172.16.0.0
 neighbor 172.16.2.3 remote-as 6000
 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 50000
 neighbor 172.16.2.3 remote-as 6000
```

```
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 192.168.0.0 (that is, if a route with any mask exists, such as 255.255.255.0 or 255.255.0.0):

```
router bgp 50000
 network 172.16.0.0
 neighbor 172.16.2.3 remote-as 60000
 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 192.168.0.0 with a mask of 255.255.0.0:

```
router bgp 50000
 network 172.16.0.0
 neighbor 172.16.2.3 remote-as 60000
 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 192.168.0.0 host 255.255.255.0
```

## Related Commands

Command	Description
<b>address-family ipv4 (BGP)</b>	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.
<b>address-family vpnv4</b>	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.
<b>neighbor ebgp-multihop</b>	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 50000
 network 172.16.0.0
 neighbor 172.16.2.3 description peer with xyz.com
```

# neighbor disable-connected-check

To disable connection verification to establish an eBGP peering session with a single-hop peer that uses a loopback interface, use the **neighbor disable-connected-check** command in Address Family or Router configuration mode. To enable connection verification for eBGP peering sessions, use the **no** form of this command.

**neighbor** *ip-address* | *peer-group-name* **disable-connected-check**

**no neighbor** *ip-address* | *peer-group-name* **disable-connected-check**

## Syntax Description

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

## Defaults

A BGP routing process will verify the connection of single-hop eBGP peering session (TTL=254) to determine if the eBGP peer is directly connected to the same network segment by default. If the peer is not directly connected to same network segment, connection verification will prevent the peering session from being established.

## Command Modes

Address Family  
Router Configuration

## Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

## Usage Guidelines

The **neighbor disable-connected-check** command is used to disable the connection verification process for eBGP peering sessions that are reachable by a single hop but are configured on a loopback interface or otherwise configured with a non-directly connected IP address.

This command is required only when the **neighbor ebgp-multihop** command is configured with a TTL value of 1. The address of the single-hop eBGP peer must be reachable. The **neighbor update-source** command must be configured to allow the BGP routing process to use the loopback interface for the peering session.

## Examples

In the following example, a single-hop eBGP peering session is configured between two BGP peers that are reachable on the same network segment through a local loopback interfaces on each router:

### BGP Peer 1

```
Router(config)# interface loopback 1
Router(config-if)# ip address 10.0.0.100 255.255.255
Router(config-if)# exit
Router(config)# router bgp 64512
Router(config-router)# neighbor 192.168.0.200 remote-as 65534
```

```

Router(config-router)# neighbor 192.168.0.200 ebgp-multihop 1
Router(config-router)# neighbor 192.168.0.200 update-source loopback 2
Router(config-router)# neighbor 192.168.0.200 disable-connected-check
Router(config-router)# end

```

### BGP Peer 2

```

Router(config)# interface loopback 2
Router(config-if)# ip address 192.168.0.200 255.255.255
Router(config-if)# exit
Router(config)# router bgp 65534
Router(config-router)# neighbor 10.0.0.100 remote-as 64512
Router(config-router)# neighbor 10.0.0.100 ebgp-multihop 1
Router(config-router)# neighbor 10.0.0.100 update-source loopback 1
Router(config-router)# neighbor 10.0.0.100 disable-connected-check
Router(config-router)# end

```

### Related Commands

Command	Description
<b>neighbor</b> <b>ebgp-multihop</b>	Accepts or initiates BGP connections to external peers residing on networks that are not directly connected.
<b>neighbor</b> <b>update-source</b>	Configures Cisco IOS software to allow BGP sessions to use any operational interface for TCP connections.

# 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.
expanded-list-number		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.
<b>in</b>		Access list is applied to incoming advertisements to that neighbor.
<b>out</b>		Access list is applied to outgoing advertisements to that neighbor.

**Defaults** No BGP neighbor is specified.

**Command Modes** Address family  
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 (IP)** 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 172.16.4.1. List 39 permits the advertisement of network 10.108.0.0.

```
router bgp 50000
 network 10.108.0.0
 neighbor 172.16.4.1 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 50000
 network 10.108.0.0
 neighbor 172.16.4.1 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 10.108/16 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
<b>access-list (IP extended)</b>	Defines an extended IP access list.
<b>access-list (IP standard)</b>	Defines a standard IP access list.
<b>address-family ipv4 (BGP)</b>	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.
<b>address-family vpnv4</b>	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.
<b>ip as-path access-list</b>	Defines a BGP-related access list.
<b>neighbor filter-list</b>	Sets up a BGP filter.
<b>neighbor peer-group (creating)</b>	Creates a BGP peer group.
<b>route-map (IP)</b>	Defines the conditions for redistributing routes from one routing protocol into another.

# neighbor dmzlink-bw

To advertise the bandwidth of links that are used to exit an autonomous system, use the **neighbor dmzlink-bw** command in address family configuration mode. To disable the **BGP Link Bandwidth feature**, use the **no** form of this command.

```
neighbor {ip-address}dmzlink-bw
```

```
no neighbor {ip-address} dmzlink-bw
```

<b>Syntax Description</b>	<b>ip-address</b> The address of the neighbor router for which the bandwidth of the outbound link is advertised.								
<b>Defaults</b>	This command is disabled by default.								
<b>Command Modes</b>	Address family configuration								
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.2(2)T</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	12.2(2)T	This command was introduced.				
Release	Modification								
12.2(2)T	This command was introduced.								
<b>Usage Guidelines</b>	Use the <b>neighbor dmzlink-bw</b> command to advertise the bandwidth of links that are used to exit an autonomous system. This feature only supports single hop links over internal Border Gateway Protocol (iBGP). BGP can originate the link bandwidth community only for external BGP (eBGP) peers that are one hop away.								
<b>Examples</b>	<p>The following example advertises the bandwidth of the link to router 10.1.1.1:</p> <pre>neighbor 10.1.1.1 dmzlink-bw</pre>								
<b>Related Commands</b>	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><b>maximum-paths</b></td> <td>Controls the maximum number of parallel routes an IP routing protocol can support.</td> </tr> <tr> <td><b>maximum-paths ibgp</b></td> <td>Control the maximum number of parallel iBGP routes that can be installed in a routing table.</td> </tr> <tr> <td><b>neighbor send-community</b></td> <td>Specifies that a communities attribute should be sent to a BGP neighbor.</td> </tr> </tbody> </table>	Command	Description	<b>maximum-paths</b>	Controls the maximum number of parallel routes an IP routing protocol can support.	<b>maximum-paths ibgp</b>	Control the maximum number of parallel iBGP routes that can be installed in a routing table.	<b>neighbor send-community</b>	Specifies that a communities attribute should be sent to a BGP neighbor.
Command	Description								
<b>maximum-paths</b>	Controls the maximum number of parallel routes an IP routing protocol can support.								
<b>maximum-paths ibgp</b>	Control the maximum number of parallel iBGP routes that can be installed in a routing table.								
<b>neighbor send-community</b>	Specifies that a communities attribute should be sent to a BGP neighbor.								

# 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 50000
 neighbor 10.108.1.1 ebgp-multihop
```

Related Commands	Command	Description
	<b>neighbor advertise-map</b> <b>non-exist-map</b>	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.
	<b>neighbor peer-group (creating)</b>	Creates a BGP peer group.
	<b>network (BGP and multiprotocol BGP)</b>	Specifies the list of networks for the BGP routing process.

# neighbor fall-over

To enable Border Gateway Protocol (BGP) fast peering session deactivation for the specified neighbor, use the **neighbor fall-over** command in address-family or router configuration mode. To disable BGP fast peering session deactivation, use the **no** form of this command.

**neighbor ip-address fall-over**

**no neighbor ip-address fall-over**

## Syntax Description

<i>ip-address</i>	IP address of the BGP neighbor.
-------------------	---------------------------------

## Defaults

No default behavior or values

## Command Modes

Address family configuration  
Router Configuration

## Command History

Release	Modification
12.0(29)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.

## Usage Guidelines

The **neighbor fall-over** command is used to enable the BGP fast peering session deactivation. BGP fast peering session deactivation improves BGP convergence and response time to adjacency changes with BGP neighbors. This feature is event driven and configured on a per-neighbor basis. When this feature is enabled, BGP will monitor the peering session with the specified neighbor. Adjacency changes are detected and terminated peering sessions are deactivated in between the default or configured BGP scanning interval.

## Examples

In the following example, the BGP routing process is configured to monitor and use fast peering session deactivation for the 10.0.0.1 neighbor session:

```
Router(config)# router bgp 50000
Router(config-router)# address-family ipv4
Router(config-router-af)# neighbor 10.0.0.1 remote-as 50000
Router(config-router-af)# neighbor 10.0.0.1 fall-over
Router(config-router-af)# end
```

## Related Commands

Command	Description
<b>bgp nexthop trigger enable</b>	Enables or disables BGP next-hop address tracking
<b>bgp nexthop trigger delay</b>	Configures the delay interval between routing table walks for BGP next-hop address tracking.

# 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 <b>ip as-path access-list</b> command.
<b>in</b>		Access list applied to incoming routes.
<b>out</b>		Access list applied to outgoing routes.

**Defaults** No filter is used.

**Command Modes** Address family  
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 <b>weight</b> 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 6000:

```
ip as-path access-list 1 deny _6000_
ip as-path access-list 1 deny ^6000$
```

```

router bgp 50000
 network 10.108.0.0
 neighbor 192.168.6.6 remote-as 6000
 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 _6000_
ip as-path access-list 1 deny ^6000$

router bgp 50000
 address-family ipv4 unicast
  network 10.108.0.0
  neighbor 192.168.6.6 remote-as 6000
  neighbor 172.16.1.1 remote-as 47
  neighbor 172.16.1.1 filter-list 1 out

```

#### Related Commands

Command	Description
<b>address-family ipv4 (BGP)</b>	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.
<b>address-family vpnv4</b>	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.
<b>ip as-path access-list</b>	Defines a BGP-related access list.
<b>match as-path</b>	Match BGP autonomous system path access lists.
<b>neighbor distribute-list</b>	Distributes BGP neighbor information as specified in an access list.
<b>neighbor peer-group (creating)</b>	Creates a BGP peer group.
<b>neighbor weight</b>	Assigns a weight to a neighbor connection.
<b>set weight</b>	Specifies the BGP weight for the routing table

# neighbor inherit peer-policy

To send a peer policy template to a neighbor so that the neighbor can inherit the configuration, use the **neighbor inherit peer-policy** command in address family or router configuration mode. To stop sending the peer policy template, use the **no** form of this command.

**neighbor** *ip-address* **inherit peer-policy** *policy-template-name*

**no neighbor** *ip-address* **inherit peer-policy** *policy-template-name*

## Syntax Description

<i>ip-address</i>	IP address of the neighbor.
<i>policy-template-name</i>	Name or tag for the peer policy template.

## Defaults

No default behavior or values

## Command Modes

Address family  
Router configuration

## Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

## Usage Guidelines

This command is used to send locally configured policy templates to the specified neighbor. If the policy template is configured to inherit configurations from other peer policy templates, the specified neighbor will also indirectly inherit these configurations from the other peer policy templates. A directly applied peer policy template can directly or indirectly inherit configurations from up to seven peer policy templates. So, a total of eight peer policy templates can be applied to a neighbor or neighbor group.



### Note

A Border Gateway Protocol (BGP) neighbor cannot be configured to work with both peer groups and peer templates. A BGP neighbor can be configured to belong only to a peer group or to inherit policies only from peer templates.

## Examples

The following example configures the 10.0.0.1 neighbor in address family configuration mode to inherit the peer policy template name CUSTOMER-A. The 10.0.0.1 neighbor will also indirectly inherit the peer policy templates in CUSTOMER-A. The explicit remote-as statement is required for the neighbor inherit statement to work. If a peering is not configured, the specified neighbor will not accept the session template.

```
Router(config)# router bgp 101
Router(config-router)# neighbor 10.0.0.1 remote-as 202
```

```
Router(config-router)# address-family ipv4 unicast
Router(config-router-af)# neighbor 10.0.0.1 inherit peer-policy CUSTOMER-A
Router(config-router-af)# exit
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>exit peer-policy</b>	Exits policy-template configuration mode and enters router configuration mode.
<b>inherit peer-policy</b>	Configures a peer policy template to inherit the configuration from another peer policy template.
<b>show ip bgp neighbors</b>	Displays information about the TCP and BGP connections to neighbors.
<b>show ip bgp template peer-policy</b>	Displays locally configured peer policy templates.
<b>template peer-policy</b>	Creates a peer policy template and enters policy-template configuration mode.

# neighbor inherit peer-session

To send a peer session template to a neighbor so that the neighbor can inherit the configuration, use the **neighbor inherit peer-session** command in address family or router configuration mode. To stop sending the peer session template, use the **no** form of this command.

**neighbor** *ip-address* **inherit peer-session** *session-template-name*

**no neighbor** *ip-address* **inherit peer-session** *session-template-name*

## Syntax Description

<i>ip-address</i>	IP address of the neighbor.
<i>session-template-name</i>	Name or tag for the peer session template.

## Defaults

No default behavior or values

## Command Modes

Address family  
Router configuration

## Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

## Usage Guidelines

This command is used to send locally configured session templates to the specified neighbor. If the session template is configured to inherit configurations from other session templates, the specified neighbor will also indirectly inherit these configurations from the other session templates. A neighbor can directly inherit only one peer session template and indirectly inherit up to seven peer session templates.



### Note

A Border Gateway Protocol (BGP) neighbor cannot be configured to work with both peer groups and peer templates. A BGP neighbor can be configured to belong only to a peer group or to inherit policies only from peer templates.

## Examples

The following example configures the 172.16.0.1 neighbor to inherit the CORE1 peer session template. The 172.16.0.1 neighbor will also indirectly inherit the configuration from the peer session template named INTERNAL-BGP. The explicit remote-as statement is required for the neighbor inherit statement to work. If a peering is not configured, the specified neighbor will not accept the session template.

```
Router(config)# router bgp 101
Router(config)# neighbor 172.16.0.1 remote-as 202
Router(config-router)# neighbor 172.16.0.1 inherit peer-session CORE1
```

Related Commands	Command	Description
	<b>exit peer-session</b>	Exits session-template configuration mode and enters router configuration mode.
	<b>inherit peer-session</b>	Configures a peer session template to inherit the configuration from another peer session template.
	<b>show ip bgp neighbors</b>	Displays information about the TCP and BGP connections to neighbors.
	<b>show ip bgp template peer-session</b>	Displays locally configured peer session templates.
	<b>template peer-session</b>	Creates a peer session template and enters session-template configuration mode.

# neighbor local-as

To customize the AS\_PATH attribute for routes received from an external Border Gateway Protocol (eBGP) neighbor, use the **neighbor local-as command** in address family or router configuration mode. To disable AS\_PATH attribute customization, use the **no** form of this command.

**neighbor** *ip-address* **local-as** *as-number* [*no-prepend* [**replace-as** [**dual-as**]]]

**no neighbor** *ip-address* **local-as** *as-number*

Syntax Description		
<i>ip-address</i>		Specifies the IP address of the eBGP neighbor.
<i>as-number</i>		Specifies an autonomous-system number to prepend to the AS_PATH attribute. The range of values for this argument is any valid autonomous system number from 1 to 65535.  <b>Note</b> With this argument, you cannot specify the autonomous system number from the local BGP routing process or from the network of the remote peer.
<i>no-prepend</i>		(Optional) Does not prepend the local autonomous system number to any routes received from the eBGP neighbor.
<i>replace-as</i>		(Optional) Prepends only the local autonomous-system number to the AS_PATH attribute. The autonomous system number from the local BGP routing process is not prepended.
<i>dual-as</i>		(Optional) Configures the eBGP neighbor to establish a peering session using the real autonomous system number (from the local BGP routing process) or by using the autonomous-system number configured with the <i>ip-address</i> argument (local-as).

**Defaults** The autonomous system number from the local BGP routing process is prepended to all external routes by default, unless the **no-prepend** and/or **replace-as** keywords are configured.

**Command Modes** Address-family configuration  
Router configuration

Command History	Release	Modification
	12.0(5)S	This command was introduced.
	12.0(5)T	CLI support for address family configuration mode was added.
	12.0(18)S 12.2(8)T 12.2(14)S	The <b>no-prepend</b> keyword was added.
	12.0(27)S 12.2(25)S 12.3(11)T	The <b>replace-as</b> and <b>dual-as</b> keywords were added.

**Usage Guidelines**

The **neighbor local-as** command is used to customize the AS\_PATH attribute by adding and removing autonomous system numbers for routes received from eBGP neighbors. The configuration of this command allows a router to appear to external peers as a member of another autonomous system for the purpose of autonomous system number migration. This feature simplifies the process of changing the autonomous system number in a BGP network by allowing the network operator to migrate customers to new configurations during normal service windows without disrupting existing peering arrangements.

**Caution**

BGP prepends the autonomous system number from each BGP network that a route traverses to maintain network reachability information and to prevent routing loops. This command should be configured only for autonomous system migration, and should be deconfigured after the transition has been completed. This procedure should be attempted only by an experienced network operator. Routing loops can be created through improper configuration.

This command can be used for only true eBGP peering sessions. This command does not work for two peers in different subautonomous systems of a confederation.

This command supports individual peering sessions and configurations applied through peer groups and peer templates. If this command is applied to a group of peers, the individual peers cannot be customized.

**Examples****Local-AS Configuration Example**

The following example establishes peering between router 1 and router 2 through autonomous system 300, using the local-as feature:

**Router 1 (Local Router)**

```
router bgp 100
  address-family ipv4 unicast
    neighbor 172.16.1.1 remote-as 200
    neighbor 172.16.1.1 local-as 300
```

**Router 2 (Remote Router)**

```
router bgp 200
  address-family ipv4 unicast
    neighbor 10.0.0.1 remote-as 300
```

**No Prepend Configuration Example**

The following example configures BGP to not prepend autonomous system 500 to routes received from the 192.168.1.1 neighbor:

```
router bgp 400
  address-family ipv4 multicast
    network 192.168.0.0
    neighbor 192.168.1.1 local-as 500 no-prepend
```

**Replace-AS Configuration Example**

The following example strips private autonomous system 64512 from outbound routing updates for the 172.20.1.1 neighbor and replaces it with autonomous system 600:

```
router bgp 64512
  address-family ipv4 unicast
    neighbor 172.20.1.1 local-as 600 no-prepend replace-as
    neighbor 172.20.1.1 remove-private-as
```

### Dual-AS Configuration Example

The following examples show the configurations for two provider networks and one customer network. Router 1 belongs to autonomous system 100, and Router 2 belongs to autonomous system 200. Autonomous system 200 is being merged into autonomous system 100. This transition needs to occur without interrupting service to Router 3 in autonomous system 300 (customer network). The **neighbor local-as** command is configured on router 1 to allow Router 3 to maintain peering with autonomous system 200 during this transition. After the transition is complete, the configuration on Router 3 can be updated to peer with autonomous system 100 during a normal maintenance window or during other scheduled downtime.

#### Router 1 Configuration (Local Provider Network)

```
interface Serial3/0
 ip address 10.3.3.11 255.255.255.0
!
router bgp 100
 no synchronization
 bgp router-id 100.0.0.11
 neighbor 10.3.3.33 remote-as 300
 neighbor 10.3.3.33 local-as 200 no-prepend replace-as dual-as
```

#### Router 2 Configuration (Remote Provider Network)

```
interface Serial3/0
 ip address 10.3.3.11 255.255.255.0
!
router bgp 200
 bgp router-id 100.0.0.11
 neighbor 10.3.3.33 remote-as 300
```

#### Router 3 Configuration (Remote Customer Network)

```
interface Serial3/0
 ip address 10.3.3.33 255.255.255.0
!
router bgp 300
 bgp router-id 100.0.0.3
 neighbor 10.3.3.11 remote-as 200
```

To complete the migration after the two autonomous systems have merged, the peering session is updated on Router 3:

```
neighbor 10.3.3.11 remote-as 100
```

#### Related Commands

Command	Description
<b>neighbor remove-private-as</b>	Removes private autonomous system numbers from outbound routing updates.
<b>show ip bgp</b>	Displays entries in the BGP routing table.
<b>show ip bgp neighbors</b>	Displays information about BGP neighbors.

# 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]} [restart
restart-interval] [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 Border Gateway Protocol (BGP) peer group.
<i>maximum</i>		Maximum number of prefixes allowed from the specified neighbor. The number of prefixes that can be configured is limited only by the available system resources on a router.
<i>threshold</i>		(Optional) Integer specifying at what percentage of the <i>maximum-prefix</i> limit the router starts to generate a warning message. The range is from 1 to 100; the default is 75.
restart		(Optional) Configures the router that is running BGP to automatically reestablish a peering session that has been disabled because the maximum-prefix limit has been exceeded. The restart timer is configured with the <i>restart-interval</i> argument.
restart-interval		(Optional) Time interval (in minutes) that a peering session is reestablished. The range is from 1 to 65535 minutes.
<b>warning-only</b>		(optional) Allows the router to generate a log message when the <i>maximum-prefix limit</i> is exceeded, instead of terminating the peering session.

## Defaults

This command is disabled by default. If the *restart-interval* argument is not configured, a disabled session will stay down by default after the maximum-prefix limit is exceeded. There is no default limit on the number of prefixes that can be configured with this command. Limitations on the number of prefixes that can be configured are determined by the amount of available system resources and are configured by the network operator. Peering sessions will be disabled (by default) when the configured maximum number of prefixes has been exceeded.

## Command Modes

Router configuration

## Command History

Release	Modification
11.3	This command was introduced.
12.0(22)S	The <b>restart</b> keyword was introduced.
12.2(15)T	The <b>restart</b> keyword was integrated into Cisco IOS Release 12.2(15)T.

**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 disables the peering session (by default).

If the **restart** keyword is configured, the router will automatically reestablish the peering session at the configured time interval.

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 101
 network 172.16.0.0
 neighbor 192.168.6.6 maximum-prefix 1000
```

The following example sets the maximum number of prefixes allowed from the neighbor at 192.168.6.6 to 50000 and configures the router to display warning messages when the router reaches 25000 prefixes or 50 percent of the maximum-prefix limit:

```
router bgp 101
 network 172.16.0.0
 neighbor 192.168.6.6 maximum-prefix 50000 50
```

The following example sets the maximum number of prefixes allowed from the neighbor at 192.168.6.6 to 2000 and configures the router to reestablish a peering session after 30 minutes if one has been disabled:

```
router bgp 101
 network 172.16.0.0
 neighbor 192.168.6.6 maximum-prefix 2000 restart 30
```

The following example sets the maximum number of prefixes allowed from the neighbor at 192.168.6.6 to 500 and configures a warning to be displayed when the maximum-prefix limit has been exceeded:

```
router bgp 101
 network 172.16.0.0
 neighbor 192.168.6.6 maximum-prefix 500 warning-only
```

**Related Commands**

Command	Description
<b>clear ip bgp</b>	Resets a BGP connection using BGP soft reconfiguration.

## neighbor maximum-prefix (EIGRP)

To limit the number of prefixes that are accepted from an Enhanced Interior Gateway Routing Protocol (EIGRP) neighbor or all EIGRP neighbors, use the **neighbor maximum-prefix** command in address-family configuration mode. To disable this function, use the **no** form of this command.

### Single Neighbor Configuration CLI

**neighbor** *ip-address* **maximum-prefix** *maximum* [*threshold*] [**warning-only**]

**no neighbor** *ip-address* **maximum-prefix**

### All Neighbor Configuration CLI

**neighbor maximum-prefix** *maximum* [*threshold*] [[**dampened**] [**reset-time** *minutes*] [**restart** *minutes*] [**restart-count** *number*] | [**warning-only**]]

**no neighbor maximum-prefix**

Syntax Description	
<i>ip-address</i>	(Optional) IP address of a single peer.
<b>maximum-prefix</b> <i>maximum</i>	Maximum number of prefixes accepted. The range for this argument is a number from 1 to 4294967295.  <b>Note</b> The number of prefixes that can be configured is limited only by the available system resources on the router.
<i>threshold</i>	(Optional) Configures the router to generate syslog warning messages when the specified percentage of the <i>maximum-prefix</i> limit has been exceeded. The prefix percentage number that can be configured for the <i>threshold</i> argument is from 1 to 100. The default is 75 percent.
<b>warning-only</b>	(Optional) Configures the router to only generate syslog messages when the <i>maximum-prefix limit</i> is reached, instead of terminating the peering session. This keyword is disabled by default.
<b>restart</b> <i>minutes</i>	(Optional) Configures a time period in which the router will not form adjacencies or accept redistributed routes from the RIB after the <i>maximum-prefix</i> limit has been exceeded. The value for the <i>minutes</i> argument is from 1 to 65535 minutes. The default restart-time period is 5 minutes.
<b>restart-count</b> <i>number</i>	(Optional) Configures the number of times a peering session can be automatically be reestablished after the peering session has been torn down or after the a redistribute route has been cleared and relearned because the <i>maximum-prefix</i> limit has been exceeded. The default restart-count limit is 3.



#### Warning

Once the restart count threshold has been crossed, you will need to enter the **clear ip route \*** or **clear ip eigrp neighbor** command to reestablish normal peering and/or redistribution.

<b>reset-time</b> <i>minutes</i>	(Optional) Configures the router to reset the restart count to 0 after the default or configured reset-time period has expired. The value for the <i>minutes</i> argument is from 1 to 65535 minutes. The default reset-time period is 15 minutes.
<b>dampened</b>	(Optional) Configures a decay penalty to be applied to the restart-time period each time the <i>maximum-prefix</i> limit is exceeded. The half-life for the decay penalty is 150% of the default or user-defined restart-time value in minutes. This keyword is disabled by default.

**Defaults**

*threshold*: 75 percent  
**reset-time**: 15 minutes  
**restart**: 5 minutes  
**restart-count**: 3

**Command Modes**

Address-family (IPv4 VRF)

**Command History**

Release	Modification
12.0(29)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.

**Usage Guidelines**

The **neighbor maximum-prefix** command can be configured to protect an individual peering session or protect all peering sessions. When this feature is enabled and the maximum-prefix limit has been exceeded, the router will tear down the peering session, clear all routes that were learned from the peer, and then place the peer in a penalty state for the default or user-defined time period. After the penalty time period expires, normal peering will be reestablished.

**Note**

In EIGRP, **neighbor** commands have been used traditionally to configure static neighbors. In the context of this feature, however, the **neighbor maximum-prefix** command can be used to configure the maximum-prefix limit for both statically configured and dynamically discovered neighbors.

When configuring the **neighbor maximum-prefix** command to protect a single peering session, only the maximum-prefix limit, the percentage threshold, the warning-only configuration options can be configured. Session dampening, restart, and reset timers are configured on a global basis

**Inherited Timer Values**

Default or user-defined **restart**, **restart-count**, and **reset-time** values for the process-level configuration of this feature, configured with the **maximum-prefix** command, are inherited by the **redistribute maximum-prefix** and **neighbor maximum-prefix** command configurations by default. If a single peer is configured with the **neighbor maximum-prefix** command, a process-level configuration or a configuration that is applied to all neighbors will be inherited.

**Examples****Configuring the Maximum Prefix Limit for a Single Peer**

The following example, starting in global configuration mode, configures the maximum prefix limit for a single peer. The maximum limit is set to 1000 prefixes, and the warning threshold is set to 80 percent. When the maximum prefix limit is exceeded, the session with this peer will be torn down, all routes learned from this peer will be removed from the topology and routing tables, and this peer will be placed in a penalty state for 5 minutes (default penalty value).

```
Router(config)# router eigrp 1
Router(config-router)# address-family ipv4 vrf RED
Router(config-router-af)# neighbor 10.0.0.1 maximum-prefix 1000 80
Router(config-router-af)# end
```

**Configuring the Maximum Prefix Limit for all Peers**

The following example, starting in global configuration mode, configures the maximum prefix limit for all peers. The maximum limit is set to 10000 prefixes, the warning threshold is set to 90 percent, the restart timer is set to 4 minutes, a decay penalty is configured for the restart timer with the **dampened** keyword, and all timers are configured to be reset to 0 every 60 minutes. When the maximum prefix limit is exceeded, all peering sessions will be torn down, all routes learned from all peers will be removed from the topology and routing tables, and all peers will be placed in a penalty state for 4 minutes (user-defined penalty value). A dampening exponential decay penalty will also be applied.

```
Router(config)# router eigrp 1
Router(config-router)# address-family ipv4 vrf RED
Router(config-router-af)# neighbor maximum-prefix 10000 90 dampened reset-time 60 restart4
Router(config-router-af)# end
```

**Related Commands**

Command	Description
<b>clear ip eigrp neighbors</b>	Deletes neighbor entries from the routing table.
<b>clear ip eigrp vrf neighbor</b>	Deletes neighbor entries from the VRF table.
<b>clear ip route</b>	Deletes routes from the IP routing table.

# 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 50000
 neighbor 10.108.1.1 next-hop-self
```

Related Commands	Command	Description
	<b>neighbor peer-group (creating)</b>	Creates a BGP peer group.
	<b>set ip next-hop (BGP)</b>	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. This command should not be configured on a route reflector, and 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
<b>address-family ipv4</b>	Enters address family configuration mode for configuring routing sessions, such as BGP, RIP, or static routing sessions, that use standard IPv4 address prefixes.
<b>address-family vpnv4</b>	Enters address family configuration mode for configuring routing sessions, such as BGP, RIP, or static routing sessions, that use standard VPNv4 address prefixes.
<b>neighbor ebgp-multihop</b>	Accepts and attempts BGP connections to external peers residing on networks that are not directly connected.
<b>neighbor route-map</b>	Applies a route map to incoming or outgoing routes.
<b>neighbor route-reflector-client</b>	Configures the router as a BGP route reflector and configures the specified neighbor as its client.

# neighbor orf prefix-filter

To advertise outbound route filter (ORF) capabilities to a peer router, use the **neighbor orf prefix-filter** command in address family or router configuration mode. To disable ORF capabilities, use the **no** form of this command.

**neighbor** *ip-address* [**capability**] **orf prefix-filter** [**receive** | **send** | **both**]

**no neighbor** *ip-address* [**capability**] **orf prefix-filter** [**receive** | **send** | **both**]

## Syntax Description

<i>ip-address</i>	The IP address of the neighbor router.
<b>capability</b>	(Optional) Informs the specified neighbor that this router has ORF capabilities.
receive	(Optional) Enables the ORF prefix list capability in receive mode.
send	(Optional) Enables the ORF prefix list capability in send mode.
both	(Optional) Enables the ORF prefix list capability in both receive and send modes.

## Defaults

This command is disabled by default.

## Command Modes

Address family  
Router configuration

## Command History

Release	Modification
12.0(11)ST	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.

## Usage Guidelines

The **neighbor prefix-filter** command is used to reduce the number of BGP prefixes that a BGP speaker sends or receives from a peer router based on prefix filtering.

In most configurations, this command will be used to advertise both send and receive ORF capabilities with the **both** keyword. However, this feature can be configured in one direction between two routers with one router configured to send ORF capabilities and another router configured to receive ORF capabilities from the first router.

## Examples

The following example configures the router to advertise ORF send capabilities to neighbor 172.16.1.2:

```
router bgp 100
  neighbor 176.16.1.2 capability orf prefix-filter send
```

The following example configures the router to advertise ORF receive capabilities to neighbor 10.1.1.1:

```
router bgp 100
```

```
neighbor 10.1.1.1 capability orf prefix-filter receive
```

The following example configures the router to advertise ORF receive capabilities to neighbor 192.168.1.2:

```
router bgp 100
  neighbor 192.168.1.2 capability orf prefix-filter both
```

---

**Related Commands**

Command	Description
<b>neighbor distribute-list</b>	Distributes BGP neighbor information as specified in an access list.
<b>neighbor prefix-list</b>	Distributes BGP neighbor information as specified in a prefix list.

# 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. 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. 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 50000
 neighbor 10.108.1.1 password bla4u00=2nkq
```

### Related Commands

Command	Description
<b>neighbor peer-group (creating)</b>	Creates a BGP peer group.

## neighbor peer-group (assigning members)

To configure a BGP neighbor to be a member of a peer group, use the **neighbor peer-group** 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  
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
<b>address-family ipv4 (BGP)</b>	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.
<b>address-family vpnv4</b>	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.
<b>neighbor peer-group (creating)</b>	Creates a BGP peer group.
<b>neighbor shutdown</b>	Disables a neighbor or peer group.

# neighbor peer-group (creating)

To create a BGP or multiprotocol BGP peer group, use the **neighbor peer-group** command in address family or router configuration mode. To remove the peer group and all of its members, use the **no** form of this command.

**neighbor** *peer-group-name* **peer-group**

**no neighbor** *peer-group-name* **peer-group**

## Syntax Description

*peer-group-name* Name of the BGP peer group.

## Defaults

There is no BGP peer group.

## Command Modes

Address family  
Router configuration

## Command History

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

## Usage Guidelines

Often in a BGP or multiprotocol BGP speaker, many neighbors are configured with the same update policies (that is, same outbound route maps, distribute lists, filter lists, update source, and so on). Neighbors with the same update policies can be grouped into peer groups to simplify configuration and make update calculation more efficient.



### Note

Peer group members can span multiple logical IP subnets, and can transmit, or pass along, routes from one peer group member to another.

Once a peer group is created with the **neighbor peer-group** command, it can be configured with the **neighbor** commands. By default, members of the peer group inherit all the configuration options of the peer group. Members also can be configured to override the options that do not affect outbound updates.

All the peer group members will inherit the current configuration as well as changes made to the peer group. Peer group members will always inherit the following configuration options by default:

- remote-as (if configured)
- version
- update-source
- outbound route-maps
- outbound filter-lists
- outbound distribute-lists
- minimum-advertisement-interval
- next-hop-self

If a peer group is not configured with a remote-as option, the members can be configured with the **neighbor** {*ip-address* | *peer-group-name*} **remote-as** command. This command allows you to create peer groups containing external BGP (eBGP) neighbors.

## Examples

The following example configurations show how to create these types of neighbor peer group:

- internal Border Gateway Protocol (iBGP) peer group
- eBGP peer group
- Multiprotocol BGP peer group

### iBGP Peer Group

In the following example, the peer group named internal configures the members of the peer group to be iBGP neighbors. By definition, this is an iBGP peer group because the **router bgp** command and the **neighbor remote-as** command indicate the same autonomous system (in this case, autonomous system 100). All the peer group members use loopback 0 as the update source and use set-med as the outbound route map. The **neighbor internal filter-list 2 in** command shows that, except for 172.16.232.55, all the neighbors have filter list 2 as the inbound filter list.

```
router bgp 100
 neighbor internal peer-group
 neighbor internal remote-as 100
 neighbor internal update-source loopback 0
 neighbor internal route-map set-med out
 neighbor internal filter-list 1 out
 neighbor internal filter-list 2 in
 neighbor 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
```

### eBGP Peer Group

The following example defines the peer group named external-peers without the **neighbor remote-as** command. By definition, this is an eBGP peer group because each individual member of the peer group is configured with its respective autonomous system number separately. Thus the peer group consists of members from autonomous systems 200, 300, and 400. All the peer group members have the set-metric route map as an outbound route map and filter list 99 as an outbound filter list. Except for neighbor 172.16.232.110, all of them have 101 as the inbound filter list.

```
router bgp 100
 neighbor external-peers peer-group
 neighbor external-peers route-map set-metric out
 neighbor external-peers filter-list 99 out
```

```

neighbor external-peers filter-list 101 in
neighbor 172.16.232.90 remote-as 200
neighbor 172.16.232.90 peer-group external-peers
neighbor 172.16.232.100 remote-as 300
neighbor 172.16.232.100 peer-group external-peers
neighbor 172.16.232.110 remote-as 400
neighbor 172.16.232.110 peer-group external-peers
neighbor 172.16.232.110 filter-list 400 in

```

### Multiprotocol BGP Peer Group

In the following example, all members of the peer group are multicast-capable:

```

router bgp 100
neighbor 10.1.1.1 remote-as 1
neighbor 172.16.2.2 remote-as 2
address-family ipv4 multicast
neighbor mygroup peer-group
neighbor 10.1.1.1 peer-group mygroup
neighbor 172.16.2.2 peer-group mygroup
neighbor 10.1.1.1 activate
neighbor 172.16.2.2 activate

```

#### Related Commands

Command	Description
<b>address-family ipv4 (BGP)</b>	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.
<b>address-family vpnv4</b>	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.
<b>clear ip bgp peer-group</b>	Removes all the members of a BGP peer group.
<b>show ip bgp peer-group</b>	Displays information about BGP peer groups.

# neighbor prefix-list

To prevent distribution of Border Gateway Protocol (BGP) neighbor information as specified in a prefix list, a Connectionless Network Service (CLNS) filter expression, or a CLNS filter set, use the **neighbor prefix-list** command in address family or router configuration mode. To remove a filter list, use the **no** form of this command.

```
neighbor {ip-address | peer-group-name} prefix-list {prefix-list-name | clns-filter-expr-name | clns-filter-set-name} {in | out}
```

```
no neighbor {ip-address | peer-group-name} prefix-list {prefix-list-name | clns-filter-expr-name | clns-filter-set-name} {in | out}
```

Syntax Description		
<i>ip-address</i>		IP address of neighbor.
<i>peer-group-name</i>		Name of a BGP peer group.
<i>prefix-list-name</i>		Name of a prefix list. This argument is used only under router configuration mode.
<i>clns-filter-expr-name</i>		Name of a CLNS filter expression. This argument is used only under network service access point (NSAP) address family configuration mode.
<i>clns-filter-set-name</i>		Name of a CLNS filter set. This argument is used only under NSAP address family configuration mode.
<b>in</b>		Filter list is applied to incoming advertisements from that neighbor.
<b>out</b>		Filter list is applied to outgoing advertisements to that neighbor.

**Defaults** All external and advertised address prefixes are distributed to BGP neighbors.

**Command Modes** Address family  
Router configuration

Command History	Release	Modification
	12.0	This command was introduced.
	12.0(7)T	Address family configuration mode was added.
	12.2(8)T	Under address family configuration mode, the <i>prefix-list-name</i> argument was amended to specify the name of a CLNS filter expression or a CLNS filter set.

**Usage Guidelines** Using prefix lists is one of three ways to filter BGP advertisements. You can also use AS-path filters, defined with the **ip as-path access-list** global configuration command and used in the **neighbor filter-list** command to filter BGP advertisements. The third way to filter BGP advertisements uses access or prefix lists with the **neighbor distribute-list** command.

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.

Use the **neighbor prefix-list** command in address family configuration mode to filter NSAP BGP advertisements.



#### 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 distribute-list** or **neighbor prefix-list**) can be applied to each inbound or outbound direction.

#### Examples

The following router configuration mode example applies the prefix list named *abc* to incoming advertisements from neighbor 10.23.4.1:

```
router bgp 65200
 network 192.168.1.2
 neighbor 10.23.4.1 prefix-list abc in
```

The following address family configuration mode example applies the prefix list named *abc* to incoming advertisements from neighbor 10.23.4.2:

```
router bgp 65001
 address-family ipv4 unicast
 network 192.168.2.4
 neighbor 10.23.4.2 prefix-list abc in
```

The following router configuration mode example applies the prefix list named *CustomerA* to outgoing advertisements to neighbor 10.23.4.3:

```
router bgp 64800
 network 192.168.3.6
 neighbor 10.23.4.3 prefix-list CustomerA out
```

The following address family configuration mode example applies the CLNS filter list set named *default-prefix-only* to outbound advertisements to neighbor 10.1.2.1:

```
clns filter-set default-prefix-only deny 49...
clns filter-set default-prefix-only permit default
!
router bgp 65202
 address-family nsap
  neighbor 10.1.2.1 activate
  neighbor 10.1.2.1 default-originate
  neighbor 10.1.2.1 prefix-list default-prefix-only out
```

#### Related Commands

Command	Description
<b>address-family ipv4 (BGP)</b>	Enters 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.
<b>address-family vpnv4</b>	Enters 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.

Command	Description
<b>clear ip prefix-list</b>	Resets the hit count of the prefix list entries.
<b>clns filter-expr</b>	Creates an entry in a CLNS filter expression.
<b>clns filter-set</b>	Creates an entry in a CLNS filter set.
<b>ip as-path access-list</b>	Defines a BGP-related access list.
<b>ip prefix-list</b>	Creates an entry in a prefix list.
<b>ip prefix-list description</b>	Adds a text description of a prefix list.
<b>ip prefix-list sequence-number</b>	Enables the generation of sequence numbers for entries in a prefix list.
<b>neighbor filter-list</b>	Sets up a BGP filter.
<b>show bgp nsap filter-list</b>	Displays information about a filter list or filter list entries.
<b>show ip bgp peer-group</b>	Displays information about BGP peer groups.
<b>show ip prefix-list</b>	Displays information about a prefix list or prefix list entries.

# neighbor remote-as

To add an entry to the BGP or multiprotocol BGP neighbor table, use the **neighbor remote-as** command in router configuration mode. To remove an entry from the table, use the **no** form of this command.

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

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

## Syntax Description

<i>ip-address</i>	IP address of the neighbor.
<i>peer-group-name</i>	Name of a BGP peer group.
<i>as-number</i>	Autonomous system to which the neighbor belongs.

## Defaults

There are no BGP or multiprotocol BGP neighbor peers.

## 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.
11.1(20)CC	The <b>nlri unicast</b> , <b>nlri multicast</b> , and <b>nlri unicast multicast</b> keywords were added.
12.0(7)T	The <b>nlri unicast</b> , <b>nlri multicast</b> , and <b>nlri unicast multicast</b> keywords were removed.

## Usage Guidelines

Specifying a neighbor with an autonomous system number that matches the autonomous system number specified in the **router bgp** global configuration command identifies the neighbor as internal to the local autonomous system. Otherwise, the neighbor is considered external.

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

By default, neighbors that are defined using the **neighbor remote-as** command in router configuration mode exchange only unicast address prefixes. To exchange other address prefix types, such as multicast and Virtual Private Network (VPN) Version 4, neighbors must also be activated using the **neighbor activate** command in address family configuration mode.

## Examples

The following example specifies that a router at the address 10.108.1.2 is a neighbor in autonomous system number 60000:

```
router bgp 50000
 network 10.108.0.0
 neighbor 10.108.1.2 remote-as 60000
```

The following example assigns a BGP router to autonomous system 50000, and two networks are listed as originating in the autonomous system. Then the addresses of three remote routers (and their autonomous systems) are listed. The router being configured will share information about networks 10.108.0.0 and 192.168.7.0 with the neighbor routers. The first router listed is in the same Class B network address space, but in a different autonomous system; the second **neighbor remote-as** command illustrates specification of an internal neighbor (with the same autonomous system number) at address 10.108.234.2; and the last **neighbor remote-as** command specifies a neighbor on a different network.

```
router bgp 50000
 network 10.108.0.0
 network 192.168.7.0
 neighbor 10.108.200.1 remote-as 167
 neighbor 10.108.234.2 remote-as 109
 neighbor 192.168.64.19 remote-as 99
```

The following example configures neighbor 10.108.1.1 in autonomous system 1 to exchange only multicast routes:

```
router bgp 50000
 neighbor 10.108.1.1 remote-as 1
 neighbor 172.31.1.2 remote-as 1
 neighbor 172.16.2.2 remote-as 2
 address-family ipv4 multicast
   neighbor 10.108.1.1 activate
   neighbor 172.31.1.2 activate
   neighbor 172.16.2.2 activate
```

The following example configures neighbor 10.108.1.1 in autonomous system 1 to exchange only unicast routes:

```
router bgp 50000
 neighbor 10.108.1.1 remote-as 1
 neighbor 172.31.1.2 remote-as 1
 neighbor 172.16.2.2 remote-as 2
```

#### Related Commands

Command	Description
<b>neighbor remote-as</b>	Creates a BGP peer group.
<b>router bgp</b>	Configures the BGP routing process.

# neighbor remove-private-as

To remove private autonomous system numbers from *t* in outbound routing updates, use the **neighbor remove-private-as** command in router configuration mode. To disable this function, use the **no** form of this command.

**neighbor** {*ip-address* | *peer-group-name*} **remove-private-as**

**no neighbor** {*ip-address* | *peer-group-name*} **remove-private-as**

## 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
10.3	This command was introduced.
11.0	The <i>peer-group-name</i> argument was added.

## Usage Guidelines

This command is available for external BGP (eBGP) neighbors only.

When an update is passed to the external neighbor, if the autonomous system path includes private autonomous system numbers, the software will drop the private autonomous system numbers.

If the autonomous system path includes both private and public autonomous system numbers, the software considers this to be a configuration error and does not remove the private autonomous system numbers.

If the autonomous system path contains the autonomous system number of the eBGP neighbor, the private autonomous system numbers will not be removed.

If this command is used with confederation, it will work as long as the private autonomous system numbers follow the confederation portion of the autonomous path.

The private autonomous system values are from 64512 to 65535.

## Examples

The following example shows a configuration that will remove the private autonomous system number from the updates sent to 172.16.2.33. The result is that the autonomous system path for the paths advertised by 10.108.1.1 through autonomous system 100 will just contain “100” (as seen by autonomous system 2051).

```
router bgp 100
  neighbor 10.108.1.1 description peer with private-as
  neighbor 10.108.1.1 remote-as 65001
  neighbor 172.16.2.33 description eBGP peer
```

```
neighbor 172.16.2.33 remote-as 2051
neighbor 172.16.2.33 remove-private-as
```

```
Router-in-AS100# show ip bgp 10.0.0.0
```

```
BGP routing table entry for 10.0.0.0/8, version 15
Paths: (1 available, best #1)
  Advertised to non peer-group peers:
    172.16.2.33
    65001
    10.108.1.1 from 10.108.1.1
      Origin IGP, metric 0, localpref 100, valid, external, best
```

```
Router-in-AS2501# show ip bgp 10.0.0.0
```

```
BGP routing table entry for 10.0.0.0/8, version 3
Paths: (1 available, best #1)
  Not advertised to any peer
    2
    172.16.2.32 from 172.16.2.32
      Origin IGP, metric 0, localpref 100, valid, external, best
```

---

**Related Commands**

Command	Description
<b>neighbor remote-as</b>	Allows entries to the BGP neighbor table.
<b>show ip bgp</b>	Displays entries in the BGP routing table.

# neighbor route-map

To apply a route map to incoming or outgoing routes, use the **neighbor route-map** command in address family or router configuration mode. To remove a route map, use the **no** form of this command.

**neighbor** {*ip-address* | *peer-group-name*} **route-map** *map-name* {**in** | **out**}

**no neighbor** {*ip-address* | *peer-group-name*} **route-map** *map-name* {**in** | **out**}

## Syntax Description

<i>ip-address</i>	IP address of the neighbor.
<i>peer-group-name</i>	Name of a BGP or multiprotocol BGP peer group.
<i>map-name</i>	Name of a route map.
<b>in</b>	Applies route map to incoming routes.
<b>out</b>	Applies route map to outgoing routes.

## Defaults

No route maps are applied to a peer.

## Command Modes

Address family  
Router configuration

## Command History

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

## Usage Guidelines

When specified in address family configuration mode, this command applies a route map to that particular address family only. When specified in router configuration mode, this command applies a route map to IP Version 4 unicast routes only.

If an outbound route map is specified, it is proper behavior to only advertise routes that match at least one section of the route map.

If you specify a BGP or multiprotocol 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.

## Examples

The following router configuration mode example applies a route map named internal-map to a BGP incoming route from 172.16.70.24:

```
router bgp 50000
 neighbor 172.16.70.24 route-map internal-map in

route-map internal-map
 match as-path 1
```

```
set local-preference 100
```

The following address family configuration mode example applies a route map named internal-map to a multiprotocol BGP incoming route from 172.16.70.24:

```
router bgp 50000
address-family ipv4 multicast
neighbor 172.16.70.24 route-map internal-map in

route-map internal-map
match as-path 1
set local-preference 100
```

#### Related Commands

Command	Description
<b>address-family ipv4 (BGP)</b>	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IP Version 4 address prefixes.
<b>address-family vpv4</b>	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPN Version 4 address prefixes.
<b>neighbor remote-as</b>	Creates a BGP peer group.

# neighbor route-reflector-client

To configure the router as a BGP route reflector and configure the specified neighbor as its client, use the **neighbor route-reflector-client** command in address family or router configuration mode. To indicate that the neighbor is not a client, use the **no** form of this command.

**neighbor** *ip-address* **route-reflector-client**

**no neighbor** *ip-address* **route-reflector-client**

## Syntax Description

*ip-address* IP address of the BGP neighbor being identified as a client.

## Defaults

There is no route reflector in the autonomous system.

## Command Modes

Address family  
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, all internal BGP (iBGP) speakers in an autonomous system must be fully meshed, and neighbors do not readvertise iBGP learned routes to neighbors, thus preventing a routing information loop. When all the clients are disabled, the local router is no longer a route reflector.

If you use route reflectors, all iBGP speakers need not be fully meshed. In the route reflector model, an Interior BGP peer is configured to be a *route reflector* responsible for passing iBGP learned routes to iBGP neighbors. This scheme eliminates the need for each router to talk to every other router.

Use the **neighbor route-reflector-client** command to configure the local router as the route reflector and the specified neighbor as one of its clients. All the neighbors configured with this command will be members of the client group and the remaining iBGP peers will be members of the nonclient group for the local route reflector.

The [bgp client-to-client reflection](#) command controls client-to-client reflection.

## Examples

In the following router configuration mode example, the local router is a route reflector. It passes learned iBGP routes to the neighbor at 172.16.70.24.

```
router bgp 50000
 neighbor 172.16.70.24 route-reflector-client
```

In the following address family configuration mode example, the local router is a route reflector. It passes learned iBGP routes to the neighbor at 172.16.70.24.

```

router bgp 50000
address-family ipv4 unicast
neighbor 172.16.70.24 route-reflector-client

```

Related Commands	Command	Description
	<b>address-family ipv4 (BGP)</b>	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IP Version 4 address prefixes.
	<b>address-family vpv4</b>	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPN Version 4 address prefixes.
	<b>bgp client-to-client reflection</b>	Restores route reflection from a BGP route reflector to clients.
	<b>bgp cluster-id</b>	Configures the cluster ID if the BGP cluster has more than one route reflector.
	<b>neighbor route-reflector-client</b>	Configures the router as a BGP route reflector and configures the specified neighbor as its client.
	<b>show ip bgp</b>	Displays entries in the BGP routing table.

# neighbor send-community

To specify that a communities attribute should be sent to a BGP neighbor, use the **neighbor send-community** command in address family or router configuration mode. To remove the entry, use the **no** form of this command.

**neighbor** {*ip-address* | *peer-group-name*} *send-community* [**both** | **standard** | **extended**]

**no neighbor** {*ip-address* | *peer-group-name*} **send-community**

## Syntax Description

<i>ip-address</i>	IP address of the neighbor.
<i>peer-group-name</i>	Name of a BGP peer group.
both	(Optional) Specifies that both standard and extended communities will be sent.
standard	(Optional) Specifies that only standard communities will be sent.
extended	(Optional) Specifies that only extended communities will be sent.

No communities attribute is sent to any neighbor.

## Command Modes

Address family  
Router configuration

## Command History

Release	Modification
10.3	This command was introduced.
11.0	The <i>peer-group-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.

## Examples

In the following router configuration mode example, the router belongs to autonomous system 50000 and is configured to send the communities attribute to its neighbor at IP address 172.16.70.23:

```
router bgp 50000
 neighbor 172.16.70.23 send-community
```

In the following address family configuration mode example, the router belongs to autonomous system 50000 and is configured to send the communities attribute to its neighbor at IP address 172.16.70.23:

```
router bgp 50000
 address-family ipv4 multicast
 neighbor 172.16.70.23 send-community
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>address-family ipv4 (BGP)</b>	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IP Version 4 address prefixes.
<b>address-family vpnv4</b>	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPN Version 4 address prefixes.
<b>match community</b>	Matches a BGP community.
<b>neighbor remote-as</b>	Creates a BGP peer group.
<b>set community</b>	Sets the BGP communities attribute.

# neighbor shutdown

To disable a neighbor or peer group, use the **neighbor shutdown** command in router configuration mode. To reenable the neighbor or peer group, use the **no** form of this command.

**neighbor** {*ip-address* / *peer-group-name*} **shutdown**

**no neighbor** {*ip-address* / *peer-group-name*} **shutdown**

## Syntax Description

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

## Defaults

No change is made to the status of any BGP neighbor or peer group.

## Command Modes

Router configuration

## Command History

Release	Modification
12.0	This command was introduced.

## Usage Guidelines

The **neighbor shutdown** command terminates any active session for the specified neighbor or peer group and removes all associated routing information. In the case of a peer group, a large number of peering sessions could be terminated suddenly.

To display a summary of BGP neighbors and peer group connections, use the [show ip bgp summary](#) command. Those neighbors with an Idle status and the Admin entry have been disabled by the [neighbor shutdown](#) command.

“State/PfxRcd” shows the current state of the BGP session or the number of prefixes the router has received from a neighbor or peer group. When the maximum number (as set by the [neighbor maximum-prefix](#) command) is reached, the string “PfxRcd” appears in the entry, the neighbor is shut down, and the connection is idle.

## Examples

The following example disables any active session for the neighbor 172.16.70.23:

```
neighbor 172.16.70.23 shutdown
```

The following example disables all peering sessions for the peer group named internal:

```
neighbor internal shutdown
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>neighbor maximum-prefix</b>	Controls how many prefixes can be received from a neighbor.
<b>show ip bgp summary</b>	Displays the status of all BGP connections.

# neighbor soft-reconfiguration

To configure the Cisco IOS software to start storing updates, use the **neighbor soft-reconfiguration** command in router configuration mode. To not store received updates, use the **no** form of this command.

**neighbor** {*ip-address* | *peer-group-name*} **soft-reconfiguration** [**inbound**]

**no neighbor** {*ip-address* | *peer-group-name*} **soft-reconfiguration** [**inbound**]

## Syntax Description

<i>ip-address</i>	IP address of the BGP-speaking neighbor.
<i>peer-group-name</i>	Name of a BGP peer group.
<b>inbound</b>	(Optional) Indicates that the update to be stored is an incoming update.

## Defaults

Soft reconfiguration is not enabled.

## Command Modes

Router configuration

## Command History

Release	Modification
11.2	This command was introduced.

## Usage Guidelines

Entering this command starts the storage of updates, which is required to do inbound soft reconfiguration. Outbound BGP soft reconfiguration does not require inbound soft reconfiguration to be enabled.

To use soft reconfiguration, or soft reset, without preconfiguration, both BGP peers must support the soft route refresh capability, which is advertised in the open message sent when the peers establish a TCP session. Routers running Cisco IOS software releases prior to Release 12.1 do not support the route refresh capability and must clear the BGP session using the **neighbor soft-reconfiguration** command. Clearing the BGP session using the **neighbor soft-reconfiguration** command has a negative effect on network operations and should only be used as a last resort. Routers running Cisco IOS software Release 12.1 or later releases support the route refresh capability and dynamic soft resets, and can use the **clear ip bgp** {*\** | *address* | *peer-group name*} **in** command to clear the BGP session.

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 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 example enables inbound soft reconfiguration for the neighbor 10.108.1.1. All the updates received from this neighbor will be stored unmodified, regardless of the inbound policy. When inbound soft reconfiguration is done later, the stored information will be used to generate a new set of inbound updates.

```
router bgp 100
 neighbor 10.108.1.1 remote-as 200
 neighbor 10.108.1.1 soft-reconfiguration inbound
```

Related Commands	Command	Description
	<b>clear ip bgp</b>	Resets a BGP connection using BGP soft reconfiguration.
	<b>neighbor remote-as</b>	Creates a BGP peer group.
	<b>show ip bgp neighbors</b>	Display information about the TCP and BGP connections to neighbors.

# neighbor timers

To set the timers for a specific BGP peer or peer group, use the **neighbor timers** command in router configuration mode. To clear the timers for a specific BGP peer or peer group, use the **no** form of this command.

**neighbor** [*ip-address* | *peer-group-name*] **timers** *keepalive holdtime*

**no neighbor** [*ip-address* | *peer-group-name*] **timers** *keepalive holdtime*

Syntax Description		
	<i>ip-address</i>	(Optional) A BGP peer or peer group IP address.
	<i>peer-group-name</i>	(Optional) Name of the BGP peer group.
	<i>keepalive</i>	Frequency (in seconds) with which the Cisco IOS software sends <i>keepalive</i> messages to its peer. The default is 60 seconds. The range is from 0 to 65535.
	<i>holdtime</i>	Interval (in seconds) after not receiving a <i>keepalive</i> message that the software declares a peer dead. The default is 180 seconds. The range is from 0 to 65535.

## Defaults

*keepalive*: 60 seconds

*holdtime*: 180 seconds

## Command Modes

Router configuration

## Command History

Release	Modification
12.0	This command was introduced.

## Usage Guidelines

The timers configured for a specific neighbor or peer group override the timers configured for all BGP neighbors using the **timers bgp** command.

## Examples

The following example changes the keepalive timer to 70 seconds and the hold-time timer to 210 seconds for the BGP peer 192.168.47.0:

```
router bgp 50000
 neighbor 192.168.47.0 timers 70 210
```

# neighbor ttl-security

To secure a Border Gateway Protocol (BGP) peering session and to configure the maximum number of hops that separate two external BGP (eBGP) peers, use the **neighbor ttl-security** command in address-family or router configuration mode. To disable this feature, use the **no** form of this command.

**neighbor** *neighbor-address* **ttl-security hops** *hop-count*

**no neighbor** *neighbor-address* **ttl-security hops** *hop-count*

## Syntax Description

<i>neighbor-address</i>	IP address of the neighbor.
<i>hops hop-count</i>	Number of hops that separate the eBGP peers. The TTL value is calculated by the router from the configured <i>hop-count</i> argument. The value for the <i>hop-count</i> argument is a number between 1 and 254.

## Defaults

No default behavior or values

## Command Modes

Address-family configuration  
Router configuration

## Command History

Release	Modification
12.0(27)S	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

## Usage Guidelines

The **neighbor ttl-security** command provides a lightweight security mechanism to protect BGP peering sessions from CPU utilization-based attacks. These types of attacks are typically brute force Denial of Service (DoS) attacks that attempt to disable the network by flooding the network with IP packets that contain forged source and destination IP addresses in the packet headers.

This feature leverages designed behavior of IP packets by accepting only IP packets with a TTL count that is equal to or greater than the locally configured value. Accurately forging the TTL count in an IP packet is generally considered to be impossible. Accurately forging a packet to match the TTL count from a trusted peer is not possible without internal access to the source or destination network.

This feature should be configured on each participating router. It secures the BGP session in the incoming direction only and has no effect on outgoing IP packets or the remote router. When this feature is enabled, BGP will establish or maintain a session only if the TTL value in the IP packet header is equal to or greater than the TTL value configured for the peering session. This feature has no effect on the BGP peering session, and the peering session can still expire if keepalive packets are not received. If the TTL value in a received packet is less than the locally configured value, the packet is silently discarded and no Internet Control Message Protocol (ICMP) message is generated. This is designed behavior; a response to a forged packet is not necessary.

To maximize the effectiveness of this feature, the *hop-count* value should be strictly configured to match the number of hops between the local and external network. However, you should also take path variation into account when configuring this feature for a multihop peering session.

The following restrictions apply to the configuration of this command:

- This feature is not supported for internal BGP (iBGP) peers or iBGP peer groups.
- The **neighbor ttl-security** command cannot be configured for a peer that is already configured with the **neighbor ebgp-multihop** command. The configuration of these commands is mutually exclusive, and only one of these commands is needed to enable a multihop eBGP peering session. An error message will be displayed in the console if you attempt to configure both commands for the same peering session.
- The effectiveness of this feature is reduced in large-diameter multihop peerings. In the event of a CPU utilization-based attack against a BGP router that is configured for large-diameter peering, you may still need to shut down the affected peering sessions to handle the attack.
- This feature is not effective against attacks from a peer that has been compromised inside of your network. This restriction also includes peers that are on the network segment between the source and destination network.

### Examples

The following example sets the hop count to 2 for a directly connected neighbor. Because the *hop-count* argument is set to 2, BGP will accept only IP packets with a TTL count in the header that is equal to or greater than 253. If a packet is received with any other TTL value in the IP packet header, the packet will be silently discarded.

```
neighbor 10.0.0.1 ttl-security hops 2
```

### Related Commands

Command	Description
<b>neighbor</b>	Accepts or initiates BGP connections to external peers residing on networks that are not directly connected.
<b>ebgp-multihop</b>	
<b>show ip bgp neighbors</b>	Displays information about the TCP and BGP connections to neighbors.

# neighbor unsuppress-map

To selectively advertise routes previously suppressed by the [aggregate-address](#) command, use the **neighbor unsuppress-map** command in address family or router configuration mode. To restore the system to the default condition, use the **no** form of this command.

**neighbor** {*ip-address* | *peer-group-name*} **unsuppress-map** *route-map-name*

**no neighbor** {*ip-address* | *peer-group-name*} **unsuppress-map** *route-map-name*

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>route-map-name</i>	Name of a route map.

**Defaults** No routes are unsuppressed.

**Command Modes** Address family  
Router configuration

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

**Usage Guidelines** Use of the **neighbor unsuppress-map** command allows specified suppressed routes to be advertised.

**Examples** The following address family configuration example shows the routes specified by a route map named *internal-map* being unsuppressed for neighbor 172.16.16.6:

```
router bgp 50000
address-family ipv4 multicast
network 172.16.0.0
neighbor 172.16.16.6 unsuppress-map internal-map
```

The following router configuration example shows the routes specified by a route map named *internal-map* being unsuppressed for neighbor 172.16.16.6:

```
router bgp 50000
network 172.16.0.0
neighbor 172.16.16.6 unsuppress-map internal-map
```

## Related Commands

Command	Description
<b>address-family ipv4 (BGP)</b>	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.
<b>address-family vpnv4</b>	Places the routing in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
<b>aggregate-address</b>	Creates an aggregate entry in a BGP routing table.
<b>neighbor route-map</b>	Applies a route map to inbound or outbound routes.

# neighbor update-source

To have the Cisco IOS software allow BGP sessions to use any operational interface for TCP connections, use the **neighbor update-source** command in router configuration mode. To restore the interface assignment to the closest interface, which is called the best local address, use the **no** form of this command.

```
neighbor {ip-address | ipv6-address | peer-group-name} update-source interface-type
interface-number
```

```
no neighbor {ip-address | ipv6-address | peer-group-name} update-source interface-type
interface-number
```

Syntax Description		
<i>ip-address</i>		IPv4 address of the BGP-speaking neighbor.
<i>ipv6-address</i>		IPv6 address of the BGP-speaking neighbor.
		This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
<i>peer-group-name</i>		Name of a BGP peer group.
<i>interface-type</i>		Interface type.
<i>interface-number</i>		Interface number.

**Defaults** Best local address

**Command Modes** Router configuration

Command History	Release	Modification
	10.0	This command was introduced.
	12.2(4)T	The <i>ipv6-address</i> argument was added.
	12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
	12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
	12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.

**Usage Guidelines** This feature can work in conjunction with the loopback interface feature described in the “Interface Configuration Overview” chapter of the Release 12.3, *Cisco IOS Interface and Hardware Component Configuration Guide*.

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.

The **neighbor update-source** command must be used to enable IPv6 link-local peering for internal or external BGP sessions.

**Examples**

The following example sources BGP TCP connections for the specified neighbor with the IP address of the loopback interface rather than the best local address:

```
router bgp 50000
 network 172.16.0.0
 neighbor 172.16.2.3 remote-as 6000
 neighbor 172.16.2.3 update-source Loopback0
```

The following example sources IPv6 BGP TCP connections for the specified neighbor in autonomous system 110 with the global IPv6 address of loopback interface 0 and the specified neighbor in autonomous system 120 with the link-local IPv6 address of Fast Ethernet interface 0/0:

```
router bgp 50000
 neighbor 3ffe::3 remote-as 110
 neighbor 3ffe::3 update-source Loopback0
 neighbor fe80::2 remote-as 120
 neighbor fe80::2 update-source FastEthernet 0/0

address-family ipv6
 neighbor 3ffe::3 activate
 neighbor fe80::2 activate
 exit-address-family
```

**Related Commands**

Command	Description
<b>neighbor activate</b>	Enables the exchange of information with a BGP neighboring router.
<b>neighbor remote-as</b>	Adds an entry to the BGP or multiprotocol BGP neighbor table.

# neighbor version

To configure the Cisco IOS software to accept only a particular BGP version, use the **neighbor version** command in router configuration mode. To use the default version level of a neighbor, use the **no** form of this command.

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

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

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>number</i>	BGP version number. The version can be set to 2 to force the software to use only Version 2 with the specified neighbor. The default is to use Version 4 and dynamically negotiate down to Version 2 if requested.

**Defaults** BGP Version 4

**Command Modes** Router configuration

Command History	Release	Modification
	10.0	This command was introduced.

**Usage Guidelines** Entering this command disables dynamic version negotiation.



**Note**

The Cisco implementation of BGP in Cisco IOS Release 12.0(5)T or earlier releases supports BGP Versions 2, 3, and 4, with dynamic negotiation down to Version 2 if a neighbor does not accept BGP Version 4 (the default version).

The Cisco implementation of BGP in Cisco IOS Release 12.0(6)T or later releases supports BGP Version 4 only and does not support dynamic negotiation down to Version 2.

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 example locks down to Version 4 of the BGP protocol:

```
router bgp 50000
 neighbor 172.16.27.2 version 4
```

Related Commands

Command	Description
<b>neighbor remote-as</b>	Creates a BGP peer group.

# neighbor weight

To assign a weight to a neighbor connection, use the **neighbor weight** command in address family or router configuration mode. To remove a weight assignment, use the **no** form of this command.

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

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

Syntax Description		
	<i>ip-address</i>	IP address of the neighbor.
	<i>peer-group-name</i>	Name of a BGP peer group.
	<i>number</i>	Weight to assign. Acceptable values are from 0 to 65535.

**Defaults** Routes learned through another BGP peer have a default weight of 0 and routes sourced by the local router have a default weight of 32768.

**Command Modes** Address family  
Router configuration

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

**Usage Guidelines** All routes learned from this neighbor will have the assigned weight initially. The route with the highest weight will be chosen as the preferred route when multiple routes are available to a particular network. The weights assigned with the **set weight** route-map command override the weights assigned using the **neighbor weight** command.



**Note**

For weight changes to take effect, use of the **clear ip bgp peer-group \*** command may be necessary.

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 weight of all routes learned via 172.16.12.1 to 50:

```
router bgp 50000
 neighbor 172.16.12.1 weight 50
```

The following address family configuration mode example sets the weight of all routes learned via 172.16.12.1 to 50:

```
router bgp 50000
address-family ipv4 multicast
neighbor 172.16.12.1 weight 50
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>address-family ipv4 (BGP)</b>	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IP Version 4 address prefixes.
<b>address-family vpv4</b>	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard Virtual Private Network (VPN) Version 4 address prefixes.
<b>neighbor distribute-list</b>	Distributes BGP neighbor information as specified in an access list.
<b>neighbor filter-list</b>	Sets up a BGP filter.
<b>neighbor remote-as</b>	Creates a BGP peer group.

# net

To configure an IS-IS network entity title (NET) for a Connectionless Network Service (CLNS) routing process, use the **net** command in router configuration mode. To remove a NET, use the **no** form of this command.

**net** *network-entity-title*

**no net** *network-entity-title*

<b>Syntax Description</b>	<i>network-entity-title</i>	NET that specifies the area address and the system ID for a CLNS routing process. This argument can be either an address or a name.
---------------------------	-----------------------------	---

<b>Defaults</b>	No NET is configured and the CLNS process will not start. A NET is mandatory.
-----------------	---

<b>Command Modes</b>	Router configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	10.0	This command was introduced.
	12.0(5)T	This command was modified to include multiarea IS-IS routing.

<b>Usage Guidelines</b>	Under most circumstances, one and only one NET must be configured.
-------------------------	--

A NET is a network service access point (NSAP) where the last byte is always zero. On a Cisco router running IS-IS, a NET can be 8 to 20 bytes. The last byte is always the n-selector and must be zero.

The six bytes directly in front of the n-selector are the system ID. The system ID length is a fixed size and cannot be changed. The system ID must be unique throughout each area (Level 1) and throughout the backbone (Level 2).

All bytes in front of the system ID are the area ID.

Even when IS-IS is used to perform IP routing only (no CLNS routing enabled), a NET must still be configured to define the router system ID and area ID.

A maximum of three NETs per router are allowed. In rare circumstances, it is possible to configure two or three NETs. In such a case, the area this router is in will have three area addresses. There will still be only one area, but it will have an additional maximum of three area addresses.

Configuring multiple NETs can be temporarily useful in the case of network reconfiguration where multiple areas are merged, or where one area is split into additional areas. Multiple area addresses enable you to renumber an area individually as needed.

If you are configuring multiarea IS-IS, the area ID must be unique, but the system ID portion of the NET must be the same for all IS-IS routing process instances.

**Examples**

The following example configures a router with system ID 0000.0c11.1111.00 and area ID 47.0004.004d.0001:

```
router isis CHESNUT
 net 47.0004.004d.0001.0001.0c11.1111.00
```

The following example shows three IS-IS routing processes with three areas configured. Each area has a unique identifier, but the system ID is the same for all areas.

```
clns routing
.
.
.

interface Tunnel529
 ip address 10.0.0.5 255.255.255.0
 ip router isis BB
 clns router isis BB

interface Ethernet1
 ip address 10.1.1.5 255.255.255.0
 ip router isis A3253-01
 clns router isis A3253-01
!
interface Ethernet2
 ip address 10.2.2.5 255.255.255.0
 ip router isis A3253-02
 clns router isis A3253-02

.
.
.

router isis BB                                ! Defaults to "is-type level-1-2"
 net 49.2222.0000.0000.0005.00
!
router isis A3253-01
 net 49.0553.0001.0000.0000.0005.00
 is-type level-1
!
router isis A3253-02
 net 49.0553.0002.0000.0000.0005.00
 is-type level-1
```

**Related Commands**

Command	Description
<b>is-type</b>	Configures the routing level for an instance of the IS-IS routing process.
<b>router isis</b>	Enables the IS-IS routing protocol and specifies an IS-IS process.

## network (BGP and multiprotocol BGP)

To specify the networks to be advertised by the Border Gateway Protocol (BGP) and multiprotocol BGP routing processes, use the **network** command in address family or router configuration mode. To remove an entry from the routing table, use the **no** form of this command.

**network** {*network-number* [**mask** *network-mask*] | *nsap-prefix*} [**route-map** *map-tag*]

**no network** {*network-number* [**mask** *network-mask*] | *nsap-prefix*} [**route-map** *map-tag*]

Syntax Description		
<i>network-number</i>		Network that BGP or multiprotocol BGP will advertise.
<b>mask</b> <i>network-mask</i>		(Optional) Network or subnetwork mask with mask address.
<i>nsap-prefix</i>		Network service access point (NSAP) prefix of the Connectionless Network Service (CLNS) network that BGP or multiprotocol BGP will advertise. This argument is used only under NSAP address family configuration mode.
<b>route-map</b> <i>map-tag</i>		(Optional) Identifier of a configured route map. The route map should be examined to filter the networks to be advertised. If not specified, all networks are advertised. If the keyword is specified, but no route map tags are listed, no networks will be advertised.

**Defaults** No networks are specified.

**Command Modes** Address family  
Router configuration

Command History	Release	Modification
	10.0	This command was introduced.
	12.0	The limit of 200 network commands per BGP router was removed.
	11.1(20)CC	The <b>nlri unicast</b> , <b>nlri multicast</b> , and <b>nlri unicast multicast</b> keywords were added.
	12.0(7)T	The <b>nlri unicast</b> , <b>nlri multicast</b> , and <b>nlri unicast multicast</b> keywords were removed.  Address family configuration mode was added.
	12.2(8)T	The <i>nsap-prefix</i> argument was added to address family configuration mode.

**Usage Guidelines** BGP and multiprotocol BGP networks can be learned from connected routes, from dynamic routing, and from static route sources.

The maximum number of **network** commands you can use is determined by the resources of the router, such as the configured NVRAM or RAM.

**Examples**

The following example sets up network 10.108.0.0 to be included in the BGP updates:

```
router bgp 65100
 network 10.108.0.0
```

The following example sets up network 10.108.0.0 to be included in the multiprotocol BGP updates:

```
router bgp 64800
 address family ipv4 multicast
 network 10.108.0.0
```

The following example advertises NSAP prefix 49.6001 in the multiprotocol BGP updates:

```
router bgp 64500
 address-family nsap
 network 49.6001
```

**Related Commands**

Command	Description
<b>address-family ipv4 (BGP)</b>	Enters the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IP Version 4 address prefixes.
<b>address-family vpnv4</b>	Enters 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.
<b>default-information originate (BGP)</b>	Allows the redistribution of network 0.0.0.0 into BGP.
<b>route-map (IP)</b>	Defines the conditions for redistributing routes from one routing protocol into another.
<b>router bgp</b>	Configures the BGP routing process.

## network (EIGRP)

To specify the network for an Enhanced Interior Gateway Routing Protocol (EIGRP) routing process, use the **network** command in router configuration mode. To remove an entry, use the **no** form of this command.

**network** *ip-address* [*subnet-mask*]

**no network** *ip-address* [*subnet-mask*]

Syntax Description		
	<i>ip-address</i>	IP address of the directly connected networks.
	<i>subnet-mask</i>	(Optional) Network mask.

**Defaults** No networks are specified.

**Command Modes** Address family  
Router configuration

Command History	Release	Modification
	10.0	This command was introduced.
	12.0(4)T	The <i>network-mask</i> argument was added.
	12.0(22)S	Address family support for EIGRP was added.
	12.2(15)T	Address family support for EIGRP was added.

**Usage Guidelines** When the **network** command is configured for an EIGRP routing process, the router matches one or more local interfaces. The **network** command will match only local interfaces that are configured with addresses that are within the same subnet as the address that has been configured with the **network** command. The router will then establish neighbors through the matched interfaces. There is no limit to the number of network statements (**network** commands) that can be configured on a router.

**Examples** The following example configures EIGRP autonomous system 1 and establishes neighbors through network 172.16.0.0 and 192.168.7.0:

```
router eigrp 1
 network 172.16.0.0
 network 192.168.7.0
```

# network (RIP)

To specify a list of networks for the Routing Information Protocol (RIP) routing process, use the **network** command in router configuration mode. To remove an entry, use the **no** form of this command.

**network** *ip-address*

**no network** *ip-address*

<b>Syntax Description</b>	<i>ip-address</i>	IP address of the network of directly connected networks.
---------------------------	-------------------	---

<b>Defaults</b>	No networks are specified.	
-----------------	----------------------------	--

<b>Command Modes</b>	Router configuration	
----------------------	----------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	10.0	This command was introduced.

**Usage Guidelines**

The network number specified must not contain any subnet information. There is no limit to the number of **network** commands you can use on the router. RIP routing updates will be sent and received only through interfaces on this network.

RIP sends updates to the interfaces in the specified networks. Also, if the network of an interface is not specified, the interface will not be advertised in any RIP update.

**Examples**

The following example defines RIP as the routing protocol to be used on all interfaces connected to networks 10.99.0.0 and 192.168.7.0:

```
router rip
 network 10.99.0.0
 network 192.168.7.0
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>router rip</b>	Configures the RIP routing process.

## network area

To define the interfaces on which OSPF runs and to define the area ID for those interfaces, use the **network area** command in router configuration mode. To disable OSPF routing for interfaces defined with the *address wildcard-mask* pair, use the **no** form of this command.

**network** *ip-address wildcard-mask area area-id*

**no network** *ip-address wildcard-mask area area-id*

Syntax Description		
	<i>ip-address</i>	IP address.
	<i>wildcard-mask</i>	IP-address-type mask that includes “don’t care” bits.
	<i>area-id</i>	Area that is to be associated with the OSPF address range. It can be specified as either a decimal value or as an IP address. If you intend to associate areas with IP subnets, you can specify a subnet address as the value of the <i>area-id</i> argument.

**Defaults** This command is disabled by default.

**Command Modes** Router configuration

Command History	Release	Modification
	10.0	This command was introduced.

**Usage Guidelines** The *ip-address* and *wildcard-mask* arguments together allow you to define one or multiple interfaces to be associated with a specific OSPF area using a single command. Using the *wildcard-mask* argument allows you to define one or multiple interfaces to be associated with a specific OSPF area using a single command. If you intend to associate areas with IP subnets, you can specify a subnet address as the value of the *area-id* argument.

For OSPF to operate on the interface, the primary address of the interface must be covered by the **network area** command. If the **network area** command covers only the secondary address, it will not enable OSPF over that interface.

The Cisco IOS software sequentially evaluates the *ip-address wildcard-mask* pair for each interface as follows:

1. The *wildcard-mask* argument is logically ORed with the interface IP address.
2. The *wildcard-mask* argument is logically ORed with the *ip-address* argument in the **network** command.
3. The software compares the two resulting values. If they match, OSPF is enabled on the associated interface and this interface is attached to the OSPF area specified.

There is no limit to the number of **network area** commands you can use on the router.

**Note**

Any individual interface can only be attached to a single area. If the address ranges specified for different areas overlap, the software will adopt the first area in the **network** command list and ignore the subsequent overlapping portions. In general, we recommend that you configure address ranges that do not overlap in order to avoid inadvertent conflicts.

When a more specific OSPF network range is removed, interfaces belonging to that network range will be retained and remain active if and only if a less specific network range exists.

For example, consider the following configuration:

```
router ospf 1
 network 192.168.129.16 0.0.0.3 area 20
 network 192.168.129.40 0.0.0.3 area 20
 network 192.168.129.44 0.0.0.3 area 20
 network 192.168.129.96 0.0.0.3 area 20
 network 192.168.128.0 0.0.127.255 area 20
!
```

Enter the following:

```
no network 192.168.129.40 0.0.0.3 area 20
```

Interfaces falling into the network range 192.168.129.40/0.0.0.3 will still remain active because the superset, 192.168.128.0/0.0.127.255, exists for area 20. A more specific network statement will cause interfaces belonging to that range to be removed from a different area only if a less specific network statement (superset) exists.

Consider a configuration such as the following:

```
!
router ospf 1
 network 192.168.128.0 0.0.127.255 area 20
!
```

If the following network statement is entered:

```
network 192.168.129.96 0.0.0.3 area 40
```

then interfaces belonging to range 192.168.129.96/0.0.0.3, if any, are removed from area 20 and moved to area 40. Network statements with identical ranges but with different area IDs are considered as area changes. For example, the following network statements will cause interfaces belonging to network range 192.168.129.40/0.0.0.3 to move from area 20 to area 40:

```
network 192.168.129.40 0.0.0.3 area 20
network 192.168.129.40 0.0.0.3 area 40
```

**Examples**

The following partial example initializes OSPF routing process 109, and defines four OSPF areas: 10.9.50.0, 2, 3, and 0. Areas 10.9.50.0, 2, and 3 mask specific address ranges, and area 0 enables OSPF for all other networks.

```
interface ethernet 0
 ip address 10.108.20.1 255.255.255.0
router ospf 109
 network 10.108.20.0 0.0.0.255 area 10.9.50.0
 network 10.108.0.0 0.0.255.255 area 2
 network 10.109.10.0 0.0.0.255 area 3
 network 0.0.0.0 255.255.255.255 area 0
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>router ospf</b>	Configures an OSPF routing process.

---

# network backdoor

To specify a backdoor route to a BGP-learned prefix that provides better information about the network, use the **network backdoor** command in address family or router configuration mode. To remove an address from the list, use the **no** form of this command.

**network *ip-address* backdoor**

**no network *ip-address* backdoor**

## Syntax Description

<i>ip-address</i>	IP address of the network to which you want a backdoor route.
-------------------	---

## Defaults

No network is marked as having a back door.

## Command Modes

Address family  
Router configuration

## Command History

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

## Usage Guidelines

A backdoor network is assigned an administrative distance of 200. The objective is to make Interior Gateway Protocol (IGP) learned routes preferred. A backdoor network is treated as a local network, except that it is not advertised. A network that is marked as a back door is not sourced by the local router, but should be learned from external neighbors. The BGP best path selection algorithm does not change when a network is configured as a back door.

## Examples

The following address family configuration example configures network 10.108.0.0 as a local network and network 192.168.7.0 as a backdoor network:

```
router bgp 50000
address-family ipv4 multicast
network 10.108.0.0
network 192.168.7.0 backdoor
```

The following router configuration example configures network 10.108.0.0 as a local network and network 192.168.7.0 as a backdoor network:

```
router bgp 50000
network 10.108.0.0
network 192.168.7.0 backdoor
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>address-family ipv4 (BGP)</b>	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IP Version 4 address prefixes.
<b>address-family vpnv4</b>	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPN Version 4 address prefixes.
<b>distance bgp</b>	Allows the use of external, internal, and local administrative distances that could be a better route to a node.
<b>network (BGP and multiprotocol BGP)</b>	Specifies networks to be advertised by the BGP and multiprotocol BGP routing processes.
<b>router bgp</b>	Assigns an absolute weight to a BGP network.

