BGP Commands_ C through I

clear bgp ipv6

To reset IPv6 Border Gateway Protocol (BGP) sessions, use the **clear bgp ipv6**command in privileged EXEC mode.

[1]

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.
*	Resets all current BGP sessions.
autonomous-system-number	Resets BGP sessions for BGP neighbors within the specified autonomous system.
ip-address	Resets the TCP connection to the specified IPv4 BGP neighbor and removes all routes learned from the connection from the BGP table.
ipv6-address	Resets the TCP connection to the specified IPv6 BGP neighbor and removes all routes learned from the connection from the BGP table. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
peer-group-name	Resets the TCP connection to the specified IPv6 BGP neighbor and removes all routes learned from the connection from the BGP table.
soft	(Optional) Soft reset. Does not reset the session.
in **out**	(Optional) Triggers inbound or outbound soft reconfiguration. If the **in** or **out** option is not specified, both inbound and outbound soft resets are triggered.

Command Default

No reset is initiated.

Command Modes

Privileged EXEC

1

Command History

Release	Modification
12.2(2)T	This command was introduced.
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.
12.3(2)T	The **unicast** keyword was added to Cisco IOS Release 12.3(2)T.
12.0(26)S	The **unicast** and **multicast** keywords were added to Cisco IOS Release 12.0(26)S.
12.3(4)T	The **multicast**keyword was added to Cisco IOS Release 12.3(4)T.
12.2(25)S	The **multicast**keyword was added to Cisco IOS Release 12.2(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **clear bgp ipv6**command is similar to the **clear ip bgp**command, except that it is IPv6-specific.

Use of the **clear bgp ipv6** command allows a reset of the neighbor sessions with varying degrees of severity depending on the specified keywords and arguments.

Use the **clear bgp ipv6 unicast** command to drop neighbor sessions with IPv6 unicast address prefixes.

The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the **unicast** keyword is mandatory starting with Cisco IOS Release 12.3(2)T.

The **multicast**keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Use the **clear bgp ipv6 *** command to drop all neighbor sessions. The Cisco IOS software will then reset the neighbor connections. Use this form of the command in the following situations:

- BGP timer specification change
- BGP administrative distance changes

Use t he **clear bgp ipv6 soft out** or the **clear bgp ipv6 unicast soft out**command to drop only the outbound neighbor connections. Inbound neighbor sessions will not be reset. Use this form of the command in the following situations:

- BGP-related access lists change or get additions
- BGP-related weights change
- BGP-related distribution lists change
- BGP-related route maps change

Use the **clear bgp ipv6 soft in**or the **clear bgp ipv6 unicast soft in**command to drop only the inbound neighbor connections. Outbound neighbor sessions will not be reset. To reset inbound routing table updates dynamically for a neighbor, you must configure the neighbor to support the router refresh capability. To determine whether a BGP neighbor supports this capability, use the **show bgp ipv6 neighbors** or the **show bgp ipv6 unicast neighbors**command. If a neighbor supports the route refresh capability, the following message is displayed:

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

If all BGP networking devices support the route refresh capability, use the **clear bgp ipv6** {*****| ip-*address*| *ipv6-address*| *peer-group-name*} **in** or the **clear bgp ipv6 unicast**{*****| ip-*address*| *ipv6-address*| *peer-group-name*} **in**command. Use of the **soft** keyword is not required when the route refresh capability is supported by all BGP networking devices, because the software automatically performs a soft reset.

Use this form of the command in the following situations:

- BGP-related access lists change or get additions
- BGP-related weights change
- BGP-related distribution lists change
- BGP-related route maps change

Examples

The following example clears the inbound session with the neighbor 7000::2 without the outbound session being reset:

```
Router# clear bgp ipv6 unicast 7000::2 soft in
```

The following example uses the **unicast** keyword and clears the inbound session with the neighbor 7000::2 without the outbound session being reset:

```
Router# clear bgp ipv6 unicast 7000::2 soft in
```

The following example clears the outbound session with the peer group named marketing without the inbound session being reset:

```
Router# clear bgp ipv6 unicast marketing soft out
```

The following example uses the **unicast** keyword and clears the outbound session with the peer group named peer-group marketing without the inbound session being reset:

```
Router# clear bgp ipv6 unicast peer-group marketing soft out
```

Related Commands

Command	Description
show bgp ipv6	Displays entries in the IPv6 BGP routing table.

clear ip bgp

To reset Border Gateway Protocol (BGP) connections using hard or soft reconfiguration, use the **clear ip bgp** command in privileged EXEC mode.

clear ip bgp {*****| **all**| *autonomous-system-number*| *neighbor-address*| **peer-group** *group-name*} [**in [prefix-filter]**| **out**| **slow**| **soft** [**in [prefix-filter]**| **out**| **slow**]]

Syntax Description

*****	Specifies that all current BGP sessions will be reset.
all	(Optional) Specifies the reset of all address family sessions.
autonomous-system-number	Number of the autonomous system in which all BGP peer sessions will be reset. Number in the range from 1 to 65535. • In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, 4-byte autonomous system numbers are supported in the range from 65536 to 4294967295 in asplain notation and in the range from 1.0 to 65535.65535 in asdot notation. • In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, 4-byte autonomous system numbers are supported in the range from 1.0 to 65535.65535 in asdot notation only. For more details about autonomous system number formats, see the **router bgp** command.
neighbor-address	Specifies that only the identified BGP neighbor will be reset. The value for this argument can be an IPv4 or IPv6 address.
peer-group *group-name*	Specifies that only the identified BGP peer group will be reset.
in	(Optional) Initiates inbound reconfiguration. If neither the **in** nor **out** keywords are specified, both inbound and outbound sessions are reset.
prefix-filter	(Optional) Clears the existing outbound route filter (ORF) prefix list to trigger a new route refresh or soft reconfiguration, which updates the ORF prefix list.

out	(Optional) Initiates inbound or outbound reconfiguration. If neither the **in** nor **out** keywords are specified, both inbound and outbound sessions are reset.
slow	(Optional) Clears slow-peer status forcefully and moves it to original update group.
soft	(Optional) Initiates a soft reset. Does not tear down the session.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.0(2)S	This command was integrated into Cisco IOS Release 12.0(2)S, and dynamic inbound soft reset capability was added.
12.0(7)T	The dynamic inbound soft reset capability was integrated into Cisco IOS Release 12.0(7)T.
12.0(22)S	The **vpnv4** and **ipv4** keywords were added.
12.0(29)S	The **mdt** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX.
12.0(32)S12	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(24)T	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.3	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SXI1	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.

Release	Modification
Cisco IOS XE Release 2.4	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
12.2(33)SRE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
15.0(1)S	This command was modified. The **slow** keyword was added.
Cisco IOS XE 3.1S	This command was modified. The **slow** keyword was added.
15.2(1)E	This command was integrated into Cisco IOS Release 15.2(1)E.

Usage Guidelines

The **clear ip bgp** command can be used to initiate a hard reset or soft reconfiguration. A hard reset tears down and rebuilds the specified peering sessions and rebuilds the BGP routing tables. A soft reconfiguration uses stored prefix information to reconfigure and activate BGP routing tables without tearing down existing peering sessions. Soft reconfiguration uses stored update information, at the cost of additional memory for storing the updates, to allow you to apply new BGP policy without disrupting the network. Soft reconfiguration can be configured for inbound or outbound sessions.

Note Due to the complexity of some of the keywords available for the **clear ip bgp** command, some of the keywords are documented as separate commands. All of the complex keywords that are documented separately start with **clear ip bgp**. For example, for information on resetting BGP connections using hard or soft reconfiguration for all BGP neighbors in IPv4 address family sessions, refer to the **clear ip bgp ipv4** command.

Generating Updates from Stored Information

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

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

Use this command whenever any of the following changes occur:

- Additions or changes to the BGP-related access lists
- Changes to BGP-related weights
- Changes to BGP-related distribution lists
- Changes to BGP-related route maps

Dynamic Inbound Soft Reset

The route refresh capability, as defined in RFC 2918, allows the local router to reset inbound routing tables dynamically by exchanging route refresh requests to supporting peers. The route refresh capability does not store update information locally for non-disruptive policy changes. It instead relies on dynamic exchange with supporting peers. Route refresh is advertised through BGP capability negotiation. All BGP routers must support the route refresh capability.

To determine if a BGP router supports this capability, use the **show ip bgp neighbors**command. The following message is displayed in the output when the router supports the route refresh capability:

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

If all BGP routers support the route refresh capability, use the **clear ip bgp**command with the **in** keyword. You need not use the **soft** keyword, because soft reset is automatically assumed when the route refresh capability is supported.

Note After configuring a soft reset (inbound or outbound), it is normal for the BGP routing process to hold memory. The amount of memory that is held depends on the size of routing tables and the percentage of the memory chunks that are utilized. Partially used memory chunks will be used or released before more memory is allocated from the global router pool.

Examples

In the following example, a soft reconfiguration is initiated for the inbound session with the neighbor 10.100.0.1, and the outbound session is unaffected:

```
Router#
 clear ip bgp 10.100.0.1 soft in
```

In the following example, the route refresh capability is enabled on the BGP neighbor routers and a soft reconfiguration is initiated for the inbound session with the neighbor 172.16.10.2, and the outbound session is unaffected:

```
Router#
 clear ip bgp 172.16.10.2 in
```

In the following example, a hard reset is initiated for sessions with all routers in the autonomous system numbered 35700:

```
Router#
 clear ip bgp 35700
```

In the following example, a hard reset is initiated for sessions with all routers in the 4-byte autonomous system numbered 65538 in asplain notation. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, or a later release.

```
Router#
 clear ip bgp 65538
```

In the following example, a hard reset is initiated for sessions with all routers in the 4-byte autonomous system numbered 1.2 in asdot notation. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(32)S12, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, 12.4(24)T, and Cisco IOS XE Release 2.3, or a later release.

```
Router#
 clear ip bgp 1.2
```

Related Commands

Command	Description
bgp slow-peer split-update-group dynamic permanent	Moves a dynamically detected slow peer to a slow update group.
clear ip bgp ipv4	Resets BGP connections using hard or soft reconfiguration for IPv4 address family sessions.
clear ip bgp ipv6	Resets BGP connections using hard or soft reconfiguration for IPv6 address family sessions.
clear ip bgp vpnv4	Resets BGP connections using hard or soft reconfiguration for VPNv4 address family sessions.
clear ip bgp vpnv6	Resets BGP connections using hard or soft reconfiguration for VPNv6 address family sessions.
neighbor slow-peer split-update-group dynamic permanent	Moves a dynamically detected slow peer to a slow update group.
neighbor soft-reconfiguration	Configures the Cisco IOS software to start storing updates.
router bgp	Configures the BGP routing process.
show ip bgp	Displays entries in the BGP routing table.
show ip bgp neighbors	Displays information about BGP and TCP connections to neighbors.
slow-peer split-update-group dynamic permanent	Moves a dynamically detected slow peer to a slow update group.

continue

To configure a route map to go to a route-map entry with a higher sequence number, use the **continue** command in route-map configuration mode. To remove a continue clause from a route map, use the **no** form of this command.

continue [*sequence-number*]

no continue

Syntax Description

sequence-number	(Optional) Route-map sequence number. If a route-map sequence number is not specified when configuring a continue clause, the continue clause will continue to the route-map entry with the next sequence number. This behavior is referred to as an "implied continue."

Command Default

If the sequence number argument is not configured when this command is entered, the continue clause will go to the route-map entry with the next default sequence number.

If a route-map entry contains a continue clause and no match clause, the continue clause will be executed automatically.

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(31)S	Support for outbound route maps was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **continue** command supports inbound route maps only in Cisco IOS Release 12.2(18)S and prior releases. Support for both inbound and outbound route maps was introduced in Cisco IOS Release 12.0(31)S and later releases.

Route Map Operation Without Continue Clauses

A route map evaluates match clauses until a successful match occurs. After the match occurs, the route map stops evaluating match clauses and starts executing set clauses, in the order in which they were configured. If a successful match does not occur, the route map "falls through" and evaluates the next sequence number of the route map until all configured route-map entries have been evaluated or a successful match occurs. Each route-map sequence is tagged with a sequence number to identify the entry. Route-map entries are evaluated in order starting with the lowest sequence number and ending with the highest sequence number. If the route map contains only set clauses, the set clauses will be executed automatically, and the route map will not evaluate any other route-map entries.

Route Map Operation With Continue Clauses

When a continue clause is configured, the route map will continue to evaluate and execute match clauses in the specified route-map entry after a successful match occurs. The continue clause can be configured to go to (or jump to) a specific route-map entry by specifying the sequence number, or if a sequence number is not specified, the continue clause will go to the next sequence number. This behavior is called an "implied continue." If a match clause exists, the continue clause is executed only if a match occurs. If no successful matches occur, the continue clause is ignored.

Match Operations With Continue Clauses

If a match clause does not exist in the route-map entry but a continue clause does, the continue clause will be automatically executed and go to the specified route-map entry. If a match clause exists in a route-map entry, the continue clause is executed only when a successful match occurs. When a successful match occurs and a continue clause exists, the route map executes the set clauses and then goes to the specified route-map entry. If the next route map contains a continue clause, the route map will execute the continue clause if a successful match occurs. If a continue clause does not exist in the next route map, the route map will be evaluated normally. If a continue clause exists in the next route map but a match does not occur, the route map will not continue and will "fall through" to the next sequence number if one exists.

Set Operations With Continue Clauses

Set clauses are saved during the match clause evaluation process and executed after the route-map evaluation is completed. The set clauses are evaluated and executed in the order in which they were configured. Set clauses are only executed after a successful match occurs, unless the route map does not contain a match clause. The continue statement proceeds to the specified route-map entry only after configured set actions are performed. If a set action occurs in the first route map and then the same set action occurs again, with a different value, in a subsequent route-map entry, the last set action will override any previous set actions that were configured with the same **set** command.

Note A continue clause can be executed, without a successful match, if a route-map entry does not contain a match clause.

Examples

In the following example, continue clause configuration is shown.

The first continue clause in route-map entry 10 indicates that the route map will go to route-map entry 30 if a successful matches occurs. If a match does not occur, the route map will "fall through" to route-map entry 20. If a successful match occurs in route-map entry 20, the set action will be executed and the route-map will not evaluate any additional route-map entries. Only the first successful **match ip address** clause is supported.

If a successful match does not occur in route-map entry 20, the route-map will "fall through" to route-map entry 30. This sequence does not contain a match clause, so the set clause will be automatically executed and the continue clause will go to the next route-map entry because a sequence number is not specified.

If there are no successful matches, the route-map will "fall through" to route-map entry 30 and execute the set clause. A sequence number is not specified for the continue clause so route-map entry 40 will be evaluated.

```
Router(config)# route-map ROUTE-MAP-NAME permit 10

Router(config-route-map)# match ip address 1

Router(config-route-map)# match metric 10

Router(config-route-map)# set as-path prepend 10

Router(config-route-map)# continue 30

Router(config-route-map)# exit
Router(config)# route-map ROUTE-MAP-NAME permit 20

Router(config-route-map)# match ip address 2

Router(config-route-map)# match metric 20
Router(config-route-map)# set as-path prepend 10 10
Router(config-route-map)# exit
Router(config)# route-map ROUTE-MAP-NAME permit 30
Router(config-route-map)# set as-path prepend 10 10 10
Router(config-route-map)# continue

Router(config-route-map)# exit

Router(config)# route-map ROUTE-MAP-NAME permit 40
Router(config-route-map)# match community 10:1
Router(config-route-map)# set local-preference 104
Router(config-route-map)# exit
```

Related Commands

Command	Description
aggregate-address	Creates an aggregate entry in a BGP or multicast BGP database.
match as-path	Match BGP autonomous system path access lists.
match community	Matches a BGP community.
match extcommunity	Matches a BGP extended community.
match interface (IP)	Distributes routes that have their next hop out one of the interfaces specified.
match ip address	Distributes any routes that have a destination network number address permitted by a standard or extended access list, or performs policy routing on packets.

Command	Description
match ip next-hop	Redistributes any routes that have a next-hop router address passed by one of the access lists specified.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match length	Bases policy routing on the Level 3 length of a packet.
match metric (IP)	Redistributes routes with the metric specified.
match mpls-label	Redistributes routes that include MPLS labels if the routes meet the conditions specified in the route map.
match route-type (IP)	Redistributes routes of the specified type.
match tag	Redistributes routes in the routing table that match the specified tags.
neighbor default-originate	Allows a BGP speaker (the local router) to send the default route 0.0.0.0 to a neighbor for use as a default route.
neighbor route-map	Applies a route map to incoming or outgoing routes.
neighbor remote-as	Adds an entry to the BGP or multiprotocol BGP neighbor table.
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol to another, or enables policy routing.
set as-path	Modifies an autonomous system path for BGP routes.
set automatic-tag	Automatically computes the tag value in a route-map configuration.
set comm-list delete	Removes communities from the community attribute of an inbound or outbound update.
set community	Sets the BGP communities attribute.
set dampening	Sets the BGP route dampening factors.

Command	Description
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set extcommunity	Sets the BGP extended communities attribute.
set interface	Indicates where to output packets that pass a match clause of route map for policy routing.
set ip default next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing and for which the Cisco IOS software has no explicit route to a destination.
set ip default next-hop verify-availability	Configures a router to check the CDP database for the availability of an entry for the default next hop that is specified by the set ip default next-hop command.
set ip next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing.
set ip next-hop verify-availability	Configures policy routing to verify if the next hops of a route map are CDP neighbors before policy routing to those next hops.
set ip precedence	Sets the precedence value in the IP header.
set level (IP)	Indicates where to import routes.
set local-preference	Specifies a preference value for the autonomous system path.
set mpls-label	Enables a route to be distributed with an MPLS label if the route matches the conditions specified in the route map.
set next-hop	Specifies the address of the next hop.
set nlri	This command was replaced by the address-family ipv4 and address-family vpnv4 commands.
set origin (BGP)	Sets the BGP origin code.
set qos-group	Sets a group ID that can be used later to classify packets.
set tag (IP)	Sets the value of the destination routing protocol.

continue

Command	Description
set traffic-index	Defines where to output packets that pass a match clause of a route map for BGP policy accounting.
set weight	Specifies the BGP weight for the routing table.
show ip bgp	Displays entries in the BGP routing table.
show route-map	Displays all route maps configured or only the one specified.

default-metric (BGP)

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

default-metric *number*

no default-metric *number*

Syntax Description

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

Command Default

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

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

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

Command Modes

Address family configuration (config-router-af)

Router configuration (config-router)

Command History

Release	Modification
10.0	This command was introduced.
12.0(7)T	Address family configuration mode support was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **default-metric** command is used to set the metric value for routes redistributed into BGP and can be applied to any external BGP (eBGP) routes received and subsequently advertised internally to iBGP peers.

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

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

Examples

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

```
Router(config)# router bgp 50000
Router(config-router)# address-family ipv4 unicast

Router(config-router-af)# default-metric 1024
Router(config-router-af)# redistribute ospf 10
Router(config-router-af)# end
```

In the following configuration and output examples, a metric of 300 is set for eBGP routes received and advertised internally to an iBGP peer.

```
Router(config)# router bgp 65501
Router(config-router)# no synchronization
Router(config-router)# bgp log-neighbor-changes
Router(config-router)# network 172.16.1.0 mask 255.255.255.0
Router(config-router)# neighbor 172.16.1.1 remote-as 65501
Router(config-router)# neighbor 172.16.1.1 soft-reconfiguration inbound
Router(config-router)# neighbor 192.168.2.2 remote-as 65502
Router(config-router)# neighbor 192.168.2.2 soft-reconfiguration inbound
Router(config-router)# default-metric 300
Router(config-router)# no auto-summary
```

After the above configuration, some routes are received from the eBGP peer at 192.168.2.2 as shown in the output from the **show ip bgp neighbors received-routes** command.

```
Router# show ip bgp neighbors 192.168.2.2 received-routes

BGP table version is 7, local router ID is 192.168.2.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 172.17.1.0/24    192.168.2.2                            0 65502 i
```

After the received routes from the eBGP peer at 192.168.2.2 are advertised internally to iBGP peers, the output from the **show ip bgp neighbors received-routes** command shows that the metric (MED) has been set to 300 for these routes.

```
Router# show ip bgp neighbors 172.16.1.2 received-routes
BGP table version is 2, local router ID is 172.16.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
* i172.16.1.0/24    172.16.1.2               0    100      0 i
* i172.17.1.0/24    192.168.2.2            300    100      0 65502 i
Total number of prefixes 2
```

Related Commands

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

exit-peer-session

To exit session-template configuration mode and enter router configuration mode, use the **exit-peer-session** command in session-template configuration mode.

exit-peer-session

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

Session-template configuration (config-router-stmp)

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.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

In the following example, the router is configured to exit session-template configuration mode and enter router configuration mode:

```
Router(config-router-stmp)# exit-peer-session
Router(config-router)#
```

Related Commands

Command	Description
template peer-session	Creates a peer session template and enters session-template configuration mode.

ha-mode graceful-restart

To enable or disable the Border Gateway Protocol (BGP) graceful restart capability for a BGP peer session template, use the **ha-mode graceful-restart** command in peer session template configuration mode. To remove from the configuration the BGP graceful restart capability for a BGP peer session template, use the **no** form of this command.

ha-mode graceful-restart [disable]

no ha-mode graceful-restart [disable]

Syntax Description

disable	(Optional) Disables BGP graceful restart capability for a neighbor.

Command Default

BGP graceful restart is disabled.

Command Modes

Peer session template configuration (config-router-stmp)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
Cisco IOS XE 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.

Usage Guidelines

The **ha-mode graceful-restart** command is used to enable or disable the graceful restart capability for a BGP peer session template. Use the **disable** keyword to disable the graceful restart capability when graceful restart has been previously enabled for the BGP peer.

The graceful restart capability is negotiated between nonstop forwarding (NSF)-capable and NSF-aware peers in OPEN messages during session establishment. If the graceful restart capability is enabled after a BGP session has been established, the session will need to be restarted with a soft or hard reset.

The graceful restart capability is supported by NSF-capable and NSF-aware routers. A router that is NSF-capable can perform a stateful switchover (SSO) operation (graceful restart) and can assist restarting peers by holding routing table information during the SSO operation. A router that is NSF-aware functions like a router that is NSF-capable but cannot perform an SSO operation.

Peer session templates are used to group and apply the configuration of general BGP session commands to groups of neighbors that share session configuration elements. General session commands that are common for neighbors that are configured in different address families can be configured within the same peer session

template. Peer session templates are created and configured in peer session configuration mode. Only general session commands can be configured in a peer session template.

General session commands can be configured once in a peer session template and then applied to many neighbors through the direct application of a peer session template or through indirect inheritance from a peer session template. The configuration of peer session templates simplifies the configuration of general session commands that are commonly applied to all neighbors within an autonomous system.

To enable the BGP graceful restart capability globally for all BGP neighbors, use the **bgp graceful-restart**command. Use the **show ip bgp neighbors** command to verify the BGP graceful restart configuration for BGP neighbors.

Examples

The following example enables the BGP graceful restart capability for the BGP peer session template named S1 and disables the BGP graceful restart capability for the BGP peer session template named S2. The external BGP neighbor at 192.168.1.2 inherits peer session template S1, and the BGP graceful restart capability is enabled for this neighbor. Another external BGP neighbor, 192.168.3.2, is configured with the BGP graceful restart capability disabled after inheriting peer session template S2.

```
router bgp 45000
 template peer-session S1
 remote-as 40000
 ha-mode graceful-restart
 exit-peer-session
 template peer-session S2
 remote-as 50000
 ha-mode graceful-restart disable
 exit-peer-session
 bgp log-neighbor-changes
 neighbor 192.168.1.2 remote-as 40000
 neighbor 192.168.1.2 inherit peer-session S1
 neighbor 192.168.3.2 remote-as 50000
 neighbor 192.168.3.2 inherit peer-session S2
 end
```

Related Commands

Command	Description
bgp graceful-restart	Enables the BGP graceful restart capability globally for all BGP neighbors.
neighbor ha-mode graceful-restart	Enables or disables the BGP graceful restart capability for a BGP neighbor or peer group.
show ip bgp neighbors	Displays information about the TCP and BGP connections to neighbors.

ip community-list

To configure a BGP community list and to control which routes are permitted or denied based on their community values, use the **ip community-list** command in global configuration mode. To delete the community list, use the **no** form of this command.

Standard Community Lists

ip community-list {*standard*| **standard** *list-name*} {**deny**| **permit**} [*community-number*] [*AA*:*NN*] **[internet] [local-as] [no-advertise] [no-export] [gshut]**

no ip community-list {*standard*| **standard** *list-name*}

Expanded Community Lists

ip community-list {*expanded*| **expanded** *list-name*} {**deny**| **permit**} *regexp*

no ip community-list {*expanded*| **expanded** *list-name*}

Syntax Description

standard	Standard community list number from 1 to 99 to identify one or more permit or deny groups of communities.
standard *list-name*	Configures a named standard community list.
deny	Denies routes that match the specified community or communities.
permit	Permits routes that match the specified community or communities.
community-number	(Optional) 32-bit number from 1 to 4294967200. A single community can be entered or multiple communities can be entered, each separated by a space.

AA **:***NN*	(Optional) Autonomous system number and network number entered in the 4-byte new community format. This value is configured with two 2-byte numbers separated by a colon. A number from 1 to 65535 can be entered for each 2-byte number. A single community can be entered or multiple communities can be entered, each separated by a space.
internet	(Optional) Specifies the Internet community. Routes with this community are advertised to all peers (internal and external).
local-as	(Optional) Specifies the local-as community. Routes with community are advertised to only peers that are part of the local autonomous system or to only peers within a subautonomous system of a confederation. These routes are not advertised to external peers or to other subautonomous systems within a confederation.
no-advertise	(Optional) Specifies the no-advertise community. Routes with this community are not advertised to any peer (internal or external).
no-export	(Optional) Specifies the no-export community. Routes with this community are advertised to only peers in the same autonomous system or to only other subautonomous systems within a confederation. These routes are not advertised to external peers.

gshut	(Optional) Specifies the Graceful Shutdown (GSHUT) community.
expanded	Expanded community list number from 100 to 500 to identify one or more permit or deny groups of communities.
expanded *list-name*	Configures a named expanded community list.
regexp	Regular expression that is used to specify a pattern to match against an input string. **Note** Regular expressions can be used only with expanded community lists.

Command Default

BGP community exchange is not enabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.3	This command was introduced.
12.0	This command was modified. The **local-as** keyword was added.
12.0(10)S	This command was modified. Named community list support was added.
12.0(16)ST	This command was modified. Named community list support was introduced.
12.1(9)E	Named community list support was integrated into Cisco IOS Release 12.1(9)E.
12.2(8)T	Named community list support was integrated into Cisco IOS Release 12.2(8)T.
12.0(22)S	This command was modified. The maximum number of expanded community list numbers was increased from 199 to 500.
12.2(14)S	This command was modified. The maximum number of expanded community list numbers was increased from 199 to 500 and named community list support were integrated into Cisco IOS Release 12.2(14)S.

Release	Modification
12.2(15)T	This command was modified. The maximum number of expanded community list numbers was increased from 199 to 500.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.2(2)S	This command was modified. The **gshut** keyword was added.
Cisco IOS XE Release 3.6S	This command was modified. The **gshut** keyword was added.
Cisco IOS XE Release 3.7S	This command was implemented on the Cisco ASR 903 router.
15.2(4)S	This command was implemented on the Cisco ASR 7200 router.

Usage Guidelines

The **ip community-list** command is used to filter BGP routes based on one or more community values. BGP community values are configured as a 32-bit number (old format) or as a 4-byte number (new format). The new community format is enabled when the **ip bgp-community new-format** command is entered in global configuration mode. The new community format consists of a 4-byte value. The first two bytes represent the autonomous system number, and the trailing two bytes represent a user-defined network number. Named and numbered community lists are supported.

BGP community exchange is not enabled by default. The exchange of BGP community attributes between BGP peers is enabled on a per-neighbor basis with the **neighbor send-community** command. The BGP community attribute is defined in RFC 1997 and RFC 1998.

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

Use a route map to reference a community list and thereby apply policy routing or set values.

Community List Processing

Once a **permit** value has been configured to match a given set of communities, the community list defaults to an implicit deny for all other community values. Unlike an access list, it is feasible for a community list to contain only **deny** statements.

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

Standard Community Lists

Standard community lists are used to configure well-known communities and specific community numbers. A maximum of 16 communities can be configured in a standard community list. If you attempt to configure

more than 16 communities, the trailing communities that exceed the limit are not processed or saved to the running configuration file.

Expanded Community Lists

Expanded community lists are used to filter communities using a regular expression. Regular expressions are used to configure patterns to match community attributes. The order for matching using the * or + character is longest construct first. Nested constructs are matched from the outside in. Concatenated constructs are matched beginning at the left side. If a regular expression can match two different parts of an input string, it will match the earliest part first. For more information about configuring regular expressions, see the "Regular Expressions" appendix of the *Terminal Services Configuration Guide*.

Examples

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

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

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

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

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

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

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

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

In the following example, a standard community list is configured that denies routes with the GSHUT community and permits routes with the local-AS community. This example shows a logical OR condition; the first match is processed.

```
Router(config)# ip community-list 18 deny gshut
Router(config)# ip community-list 18 permit local-as
```

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

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

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

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

Related Commands

Command	Description
match community	Defines a BGP community that must match the community of a route.
neighbor send-community	Allows BGP community exchange with a neighbor.

Command	Description
neighbor shutdown graceful	Configures the BGP Graceful Shutdown feature.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set community	Sets the BGP communities attribute.
set comm-list delete	Removes communities from the community attribute of an inbound or outbound update.
show ip bgp community	Displays routes that belong to specified BGP communities.
show ip bgp regexp	Displays routes that match a locally configured regular expression.

ip extcommunity-list

To create an extended community list to configure Virtual Private Network (VPN) route filtering, use the **ip extcommunity-list** command in global configuration mode. To delete the extended community list, use the **no** form of this command.

To enter IP Extended community-list configuration mode to create or configure an extended community-list, use the **ip extcommunity-list** command in global configuration mode. To delete the entire extended community list, use the **no** form of this command. To delete a single entry, use the **no** form in IP Extended community-list configuration mode.

Global Configuration Mode CLI

ip extcommunity-list {*expanded-list* [**permit**| **deny**] [*regular-expression*]| **expanded** *list-name* [**permit**| **deny**] [*regular-expression*]| *standard-list* [**permit**| **deny**] [**rt** *value*] [**soo** *value*]| **standard** *list-name* [**permit**| **deny**] [**rt** *value*] [**soo** *value*]}

no ip extcommunity-list {*expanded-list*| **expanded** *list-name*| *standard-list*| **standard** *list-name*}

ip extcommunity-list {*expanded-list*| **expanded** *list-name*| *standard-list*| **standard** *list-name*}

no ip extcommunity-list {*expanded-list*| **expanded** *list-name*| **s** *tandard-list*| **standard** *list-name*}

Expanded IP Extended Community-List Configuration Mode CLI

[*sequence-number*] {**deny** [*regular-expression*]| **permit** [*regular-expression*]| **resequence** [*starting-sequence*] [*sequence-increment*]}

default {*sequence-number*| **deny** [*regular-expression*]| **permit** [*regular-expression*]| **resequence** [*starting-sequence*] [*sequence-increment*]}

no {*sequence-number*| **deny** [*regular-expression*]| **permit** [*regular-expression*]| **resequence** [*starting-sequence*] [*sequence-increment*]}

Standard IP Extended Community-List Configuration Mode CLI

default {*sequence-number*| **deny** [**rt** *value*] [**soo** *value*]| **permit** [**rt** *value*] [**soo** *value*]| **resequence** [*starting-sequence*] [*sequence-increment*]}

no {*sequence-number*| **deny** [**rt** *value*| **soo** *value*]| **permit** [**rt** *value*] [**soo** *value*]| **resequence** [*starting-sequence*] [*sequence-increment*]}

Syntax Description

expanded-list	An expanded list number from 100 to 500 that identifies one or more permit or deny groups of extended communities.
standard-list	A standard list number from 1 to 99 that identifies one or more permit or deny groups of extended communities.

expanded *list-name*	Creates an expanded named extended community list and enters IP Extended community-list configuration mode.
standard *list-name*	Creates a standard named extended community list and enters IP Extended community-list configuration mode.
permit	Permits access for a matching condition. Once a permit value has been configured to match a given set of extended communities, the extended community list defaults to an implicit deny for all other values.
deny	Denies access for a matching condition.
regular-expression	(Optional) An input string pattern to match against.
rt	(Optional) Specifies the route target (RT) extended community attribute. The **rt** keyword can be configured only with standard extended community lists and not expanded community lists.
soo	(Optional) Specifies the site of origin (SOO) extended community attribute. The **soo**keyword can be configured only with standard extended community lists and not expanded community lists.
value	Specifies the route target or site of origin extended community value. This value can be entered in one of the following formats: • autonomous-system-number : network-number • ip-address : network-number
sequence-number	(Optional) The sequence number of a named or numbered extended community list. This value can be a number from 1 to 2147483647.
resequence	(Optional) Changes the sequences of extended community list entries to the default sequence numbering or to the specified sequence numbering. Extended community entries are sequenced by ten number increments by default.
starting-sequence	(Optional) Specifies the number for the first entry in an extended community list.
sequence-increment	(Optional) Specifies the increment range for each subsequent extended community entry.

Command Default Extended community exchange is not enabled by default.

Command Modes Global configuration (config)

IP Extended community-list configuration (config-extcom-list)

Command History

Release	Modification
12.1	This command was introduced.
12.0(22)S	The maximum number of expanded community list numbers was increased from 199 to 500.
12.2(15)T	The maximum number of expanded community list numbers was increased from 199 to 500.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(25)S	Support for the following was added in Cisco IOS Release 12.2(25)S: • Extended community-list sequencing • IP Extended community configuration mode • Named extended community lists
12.3(11)T	Support for the following was added in Cisco IOS Release 12.3(11)T: • Extended community-list sequencing • IP Extended community configuration mode • Named extended community lists
12.2(27)SBC	This command was integrated into the Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(14)SX	This command was integrated into the Cisco IOS Release 12.2(14)SX.
12.0(32)S12	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(24)T	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.

Release	Modification
Cisco IOS XE Release 2.3	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SXI1	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
12.2(33)SRE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
Cisco IOS Release 15.1(1)SG	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
Cisco IOS XE Release 3.3SG	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
15.2(1)E	This command was integrated into the Cisco IOS Release 15.2(1)E.

Usage Guidelines

The **ip extcommunity-list** command is used to configure named or numbered extended community lists. Extended community attributes are used to filter routes for VPN routing and forwarding instances (VRFs) and Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs). All of the standard rules of access lists apply to the configuration of extended community lists. The route target (RT) and site of origin (SOO) extended community attributes are supported by the standard range of extended community lists. Extended community list entries start with the number 10 and increment by ten for each subsequent entry when no sequence number is specified, when default behavior is configured, and when an extended community list is resequenced without specifying the first entry number or the increment range for subsequent entries. Regular expressions are supported in expanded extended community lists. For information about configuring regular expressions, see the "Regular Expressions" appendix of the Cisco IOS Terminal Services Configuration Guide.

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

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

Route Target Extended Community Attribute

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

Site of Origin Extended Community Attribute

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

IP Extended Community-List Configuration Mode

Named and numbered extended community lists can be configured in IP Extended community-list configuration mode. To enter IP Extended community-list configuration mode, enter the **ip extcommunity-list** command with either the **expanded** or **standard** keyword followed by the extended community list name. This configuration mode supports all of the functions that are available in global configuration mode. In addition, you can perform the following operations:

- Configure sequence numbers for extended community list entries
- Resequence existing sequence numbers for extended community list entries
- Configure an extended community list to use default values

Extended Community List Processing

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

Examples

Examples

In the following example, an extended community list is configured that permits routes from route target 64512:10 and site of origin 65400:20 and denies routes from route target 65424:30 and site of origin 64524:40. List 1 shows a logical OR condition; the first match is processed. List 2 shows a logical AND condition; all community values must match in order for list 2 to be processed.

```
Router(config)# ip extcommunity-list 1 permit rt 64512:10
Router(config)# ip extcommunity-list 1 permit soo 65400:20
Router(config)# ip extcommunity-list 2
 deny rt 65424:30 soo 64524:40
```

Examples

In the following example, an expanded extended community list is configured to deny advertisements from any path through or from autonomous system 65534 from being advertised to the 192.168.1.2 neighbor:

```
Router(config)# ip extcommunity-list 500 deny _65412_
Router(config)# router bgp 50000
Router(config-router)# address-family vpnv4
```

```
Router(config-router-af)# neighbor 172.16.1.1 remote-as 65412
Router(config-router-af)# neighbor 172.16.1.1
 neighbor send-community extended
Router(config-router-af)# neighbor 192.168.1.2 remote-as 65534
Router(config-router-af)# neighbor 192.168.1.2
 neighbor send-community extended
Router(config-router-af)# end
```

Examples

In the following example, a named extended community list is configured that will permit routes only from route target 65505:50. All other routes are implicitly denied.

```
Router(config)# ip extcommunity-list standard NAMED_LIST permit rt 65505:50
```

Examples

In the following example, an expanded named extended community list is configured in IP Extended community-list configuration mode. A list entry is created with a sequence number 10 that will permit a route target or route origin pattern that matches any network number extended community from autonomous system 65412.

```
Router(config)# ip extcommunity-list RED
Router(config-extcom-list)# 10 permit 65412:[0-9][0-9][0-9][0-9][0-9]_
Router(config-extcom-list)# exit
```

Examples

In the following example, the first list entry is resequenced to the number 50 and each subsequent entry is configured to increment by 100:

```
Router(config)# ip extcommunity-list BLUE
Router(config-extcom-list)# resequence 50 100
Router(config-extcom-list)# exit
```

Examples

The following example shows how to filter traffic by creating an extended BGP community list to control outbound routes. In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, extended BGP communities support 4-byte autonomous system numbers in the regular expressions in asplain format. In this task, the router is configured with an extended named community list to specify that the BGP peer at 192.168.1.2 is not sent advertisements about any path through or from the 4-byte autonomous system 65550. The IP extended community-list configuration mode is used, and the ability to resequence entries is shown.

```
Router(config)# ip extcommunity-list expanded DENY65550
Router(config-extcomm-list)# 10 deny _65550_
Router(config-extcomm-list)# 20 deny ^65550 .*
Router(config-extcomm-list)# resequence 50 100
Router(config-extcomm-list)# exit
Router(config)# router bgp 65538
Router(config-router)# network 172.17.1.0 mask 255.255.255.0

Router(config-router)# neighbor 192.168.3.2 remote-as 65550
Router(config-router)# neighbor 192.168.1.2 remote-as 65536
Router(config-router)# neighbor 192.168.3.2 activate
Router(config-router)# neighbor 192.168.1.2 activate
Router(config-router)# end
Router# show ip extcommunity-list DENY65550
```

In Cisco IOS Release 12.0(32)SY8, 12.0(32)S12, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, 12.4(24)T, and Cisco IOS XE Release 2.3, or a later releases, extended BGP communities support 4-byte autonomous system numbers in the regular expressions in asdot format. In this task, the router is configured with an extended named community list to specify that the BGP peer at 192.168.1.2 is not sent advertisements about any path

through or from the 4-byte autonomous system 1.14. The IP extended community-list configuration mode is used, and the ability to resequence entries is shown.

```
Router(config)# ip extcommunity-list expanded DENY114
Router(config-extcomm-list)# 10 deny _1\.14_
Router(config-extcomm-list)# 20 deny ^1\.14 .*
Router(config-extcomm-list)# resequence 50 100
Router(config-extcomm-list)# exit
Router(config)# router bgp 1.2
Router(config-router)# network 172.17.1.0 mask 255.255.255.0
Router(config-router)# neighbor 192.168.3.2 remote-as 1.14
Router(config-router)# neighbor 192.168.1.2 remote-as 1.0
Router(config-router)# neighbor 192.168.3.2 activate
Router(config-router)# neighbor 192.168.1.2 activate
Router(config-router)# end
Router# show ip extcommunity-list DENY114
```

Related Commands

Command	Description
bgp asnotation dot	Changes the default display and regular expression match format of BGP 4-byte autonomous system numbers from asplain (decimal values) to dot notation.
export map	Configures an export route map for a VRF.
match extcommunity	Matches a BGP VPN extended community list.
router bgp	Configures the BGP routing process.
set extcommunity	Sets BGP extended community attributes.
show ip extcommunity-list	Displays routes that are permitted by the extended community list.
show route-map	Displays configured route maps.

ip prefix-list

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

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

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

Syntax Description

list-name	Configures a name to identify the prefix list. Do not use the word “detail” or “summary” as a list name because they are keywords in the **show ip prefix-list** command.
seq	(Optional) Applies a sequence number to a prefix-list entry.
number	(Optional) Integer from 1 to 4294967294. If a sequence number is not entered when configuring this command, default sequence numbering is applied to the prefix list. The number 5 is applied to the first prefix entry, and subsequent unnumbered entries are incremented by 5.
deny	Denies access for a matching condition.
permit	Permits access for a matching condition.
network / *length*	Configures the network address and the length of the network mask in bits. The network number can be any valid IP address or prefix. The bit mask can be a number from 1 to 32.
ge	(Optional) Specifies the lesser value of a range (the “from” portion of the range description) by applying the *ge-length* argument to the range specified. **Note** The **ge** keyword represents the greater than or equal to operator.
ge-length	(Optional) Represents the minimum prefix length to be matched.

le	(Optional) Specifies the greater value of a range (the "to" portion of the range description) by applying the *le-length* argument to the range specified. **Note** The **le** keyword represents the less than or equal to operator.
le-length	(Optional) Represents the maximum prefix length to be matched.
description	(Optional) Configures a descriptive name for the prefix list.
description	(Optional) Descriptive name of the prefix list, from 1 to 80 characters in length.
sequence-number	(Optional) Enables or disables the use of sequence numbers for prefix lists.

Command Default

No prefix lists or prefix-list entries are created.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **ip prefix-list** command to configure IP prefix filtering. Prefix lists are configured with **permit** or **deny** keywords to either permit or deny a prefix based on a matching condition. An implicit deny is applied to traffic that does not match any prefix-list entry.

A prefix-list entry consists of an IP address and a bit mask. The IP address can be for a classful network, a subnet, or a single host route. The bit mask is a number from 1 to 32.

Prefix lists are configured to filter traffic based on a match of an exact prefix length or a match within a range when the **ge** and **le** keywords are used. The **ge** and **le** keywords are used to specify a range of prefix lengths and provide more flexible configuration than using only the *network* / *length*argument. A prefix list is processed using an exact match when neither the **ge** nor **le** keyword is specified. If only the **ge** value is specified, the range is the value entered for the **ge** *ge-length* argument to a full 32-bit length. If only the **le** value is specified, the range is from the value entered for the *network* / *length argument*to the **le** *le-length* argument. If both the

ge *ge-length*and **le** *le-length* keywords and arguments are entered, the range is between the values used for the *ge-length* and *le-length* arguments.

The following formula shows this behavior:

length < **ge** *ge-length* < **le** *le-length* <= 32

If the **seq** keyword is configured without a sequence number, the default sequence number is 5. In this scenario, the first prefix-list entry is assigned the number 5 and subsequent prefix list entries increment by 5. For example, the next two entries would have sequence numbers 10 and 15. If a sequence number is entered for the first prefix list entry but not for subsequent entries, the subsequent entry numbers increment by 5. For example, if the first configured sequence number is 3, subsequent entries will be 8, 13, and 18. Default sequence numbers can be suppressed by entering the **no ip prefix-list**command with the **seq** keyword.

Evaluation of a prefix list starts with the lowest sequence number and continues down the list until a match is found. When an IP address match is found, the permit or deny statement is applied to that network and the remainder of the list is not evaluated.

Tip For best performance, the most frequently processed prefix list statements should be configured with the lowest sequence numbers. The **seq** *number*keyword and argument can be used for resequencing.

A prefix list is applied to inbound or outbound updates for a specific peer by entering the **neighbor prefix-list** command. Prefix list information and counters are displayed in the output of the **show ip prefix-list** command. Prefix-list counters can be reset by entering the **clear ip prefix-list** command.

Examples

In the following example, a prefix list is configured to deny the default route 0.0.0.0/0:

```
Router(config)# ip prefix-list RED deny 0.0.0.0/0
```

In the following example, a prefix list is configured to permit traffic from the 172.16.1.0/24 subnet:

```
Router(config)# ip prefix-list BLUE permit 172.16.1.0/24
```

In the following example, a prefix list is configured to permit routes from the 10.0.0.0/8 network that have a mask length that is less than or equal to 24 bits:

```
Router(config)# ip prefix-list YELLOW permit 10.0.0.0/8 le 24
```

In the following example, a prefix list is configured to deny routes from the 10.0.0.0/8 network that have a mask length that is greater than or equal to 25 bits:

```
Router(config)# ip prefix-list PINK deny 10.0.0.0/8 ge 25
```

In the following example, a prefix list is configured to permit routes from any network that have a mask length from 8 to 24 bits:

```
Router(config)# ip prefix-list GREEN permit 0.0.0.0/0 ge 8 le 24
```

In the following example, a prefix list is configured to deny any route with any mask length from the 10.0.0.0/8 network:

```
Router(config)# ip prefix-list ORANGE deny 10.0.0.0/8 le 32
```

Related Commands

Command	Description
clear ip prefix-list	Resets the prefix list entry counters.
ip prefix-list description	Adds a text description of a prefix list.
ip prefix-list sequence	Enables or disables default prefix-list sequencing.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
neighbor prefix-list	Filters routes from the specified neighbor using a prefix list.
show ip prefix-list	Displays information about a prefix list or prefix list entries.