match as-path

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

match as-path *path-list-number*

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

Syntax Description

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

Defaults

No path lists are defined.

Command Modes

Route-map configuration

Command History

Release	Modification
10.0	This command was introduced.
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 values set by the **match as-path** and **set weight** commands override global values. For example, the weights assigned with the **match as-path** and **set weight** route-map configuration commands override the weight assigned using the **neighbor weight** command.

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

Examples

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

```
route-map IGP2BGP
 match as-path 20
```

Related Commands

Command	Description
match community	Matches a BGP community.
match interface (IP)	Distributes routes that have their next hop out one of the interfaces specified.

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

match community

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

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

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

Syntax Description

standard-list-number	Specifies a standard community list number from 1 to 99 that identifies one or more permit or deny groups of communities.
expanded-list-number	Specifies an expanded community list number from 100 to 500 that identifies one or more permit or deny groups of communities.
community-list-name	The community list name.
exact	(Optional) Indicates that an exact match is required. All of the communities and only those communities specified must be present.

Command Default

No community list is matched by the route map.

Command Modes

Route-map configuration

Command History

Release	Modification
12.1	This command was introduced.
12.1(9)E	Named community list support was integrated into Cisco IOS Release 12.1(9)E.
12.2(8)T	Named community list support was integrated into Cisco IOS Release 12.2(8)T.
12.0(22)S	The maximum number of expanded extended community list numbers was changed from 199 to 500 in Cisco IOS Release 12.0(22)S.
12.2(14)S	The maximum number of expanded community lists was changed from 199 to 500 and named community list support were integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	The maximum number of expanded extended community list numbers was changed from 199 to 500 in Cisco IOS Release 12.2(15)T.
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

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

Matching based on community list number is one of the types of **match** commands applicable to BGP.

Examples

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

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

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

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

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

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

The following example shows that the routes that match expanded community list 500. Any route that has extended community 1 will have the weight set to 150.

```
Router(config)# ip community-list 500 permit [0-9]*
Router(config)# route-map MAP_NAME permit 10
Router(config-route-map)# match extcommunity 500
Router(config-route-map)# set weight 150
```

Related Commands

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

match extcommunity

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

match extcommunity *extended-community-list-name*

no match extcommunity *extended-community-list-name*

Syntax Description

extended-community-list-name	Name of an extended community list.

Command Default

BGP and EIGRP extended community list attributes are not matched.

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
12.1	This command was introduced.
12.0(22)S	The maximum number of expanded extended community list numbers was changed from 199 to 500 in Cisco IOS Release 12.0(22)S.
12.2(15)T	The maximum number of expanded extended community list numbers was changed from 199 to 500 in Cisco IOS Release 12.2(15)T.
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 integrated into Cisco IOS XE Release 2.1.
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.
15.0(1)M	This command was modified. Support for EIGRP was added.
12.2(33)SRE	This command was modified. Support for EIGRP was added.
Cisco IOS XE Release 2.5	This command was modified. Support for EIGRP was added.
12.2(33)XNE	This command was modified. Support for EIGRP was added.

Usage Guidelines

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

The **match extcommunity** command is used to configure match clauses that use extended community attributes in route maps. All of the standard rules of match and set clauses apply to the configuration of extended community attributes.

Examples

The following example shows that the routes that match extended community list 500 will have the weight set to 100. Any route that has extended community 1 will have the weight set to 100.

```
Router(config)# ip extcommunity-list 500 rt 100:2
Router(config-extcomm-list)# exit
Router(config)# route-map MAP_NAME permit 10
Router(config-route-map)# match extcommunity 1
Router(config-route-map)# set weight 100
```

Related Commands

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

match local-preference

To configure a route map to match routes based on the Border Gateway Protocol (BGP) local-preference attribute, use the **match local-preference** command in route-map configuration mode. To remove the match clause entry from the route map, use the **no** form of this command.

match local-preference *value*

no match local-preference *value*

Syntax Description

value	The local preference value. This argument can be entered as a number from 0 to 4294967295.

Command Default

Cisco IOS software uses a default value of 100 for the local-preference attribute. However, a local-preference value must be entered when configuring a match clause with this command.

Command Modes

Route-map configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)S.

Usage Guidelines

The **match local-preference** command is used to filter routes based on the value of the local preference attribute. The local-preference attribute is a well-known discretionary attribute that is used to set the preference for an exit point within an autonomous system. The route with the highest local-preference value is preferred by the BGP best path selection process.

Redistributing OER Injected Routes

Optimized Edge Routing (OER) uses a local-preference value of 5000 (default) to move traffic to the preferred exit point in a BGP network (This value can be configured on the OER master controller). The **match local-preference** command can be used to redistribute OER injected routes within an autonomous system that is monitored and controlled by OER.

Examples

The following example configures the route-map name RED to match OER injected routes:

```
Router(config)# route-map RED permit 10
Router(config-route-map)# match local-preference 5000
```

Related Commands

Command	Description
bgp default local-preference	Changes the default local-preference value.
route-map (IP)	Defines conditions for redistributing routes.
set local-preference	Applies a local-preference value to routes that pass the match clause.

match policy-list

To configure a route map to evaluate and process a Border Gateway Protocol (BGP) policy list in a route map, use the **match policy-list command in** route-map configuration mode. To remove a path list entry, use the **no** form of this command.

match policy-list *policy-list-name*

no match policy-list *policy-list-name*

Syntax Description

policy-list-name	Name of the policy list to evaluate and process within the route map.

Defaults

This command is not enabled by default.

Command Modes

Route-map configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(15)T	This command was integrated into 12.2(15)T.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.

Usage Guidelines

When a policy list is referenced within a route map, all the match statements within the policy list are evaluated and processed.

Two or more policy lists can be configured with a route map. Policy lists can be configured within a route map to be evaluated with AND semantics or OR semantics.

Policy lists can also coexist with any other preexisting match and set statements that are configured within the same route map but outside of the policy lists.

When multiple policy lists perform matching within a route map entry, all policy lists match on the incoming attribute only.

Examples

The following configuration example creates a route map that references policy lists and separate match and set clauses in the same configuration:

```
Router(config)# route-map MAP-NAME-1 10
Router(config-route-map)# match ip-address 1
Router(config-route-map)# match policy-list POLICY-LIST-NAME-1
Router(config-route-map)# set community 10:1
Router(config-route-map)# set local-preference 140
Router(config-route-map)# end
```

The following configuration example creates a route map that references policy lists and separate match and set clauses in the same configuration. This example processes the policy lists named POLICY-LIST-NAME-2 and POLICY-LIST-NAME-3 with OR semantics. A match is required from only one of the policy lists.

```
Router(config)# route-map MAP-NAME-2 10
Router(config-route-map)# match policy-list POLICY-LIST-NAME-2 POLICY-LIST-NAME-3
Router(config-route-map)# set community 10:1
Router(config-route-map)# set local-preference 140
Router(config-route-map)# end
```

Related Commands

Command	Description
ip policy-list	Creates a BGP policy list.
match as-path	References a policy list within a route map for evaluation and processing.
match community	Matches a BGP community.
match interface (IP)	Distributes routes that have their next hop out one of the interfaces specified.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match ip next-hop	Redistributes any routes that have a next hop router address passed by one of the access lists specified.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match metric (IP)	Redistributes routes with the metric specified.
match route-type (IP)	Redistributes routes of the specified type.
match tag	Redistributes routes in the routing table that match the specified tags.
neighbor weight	Assigns weight to a neighbor connection.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.

match source-protocol

To match Enhanced Interior Gateway Routing Protocol (EIGRP) external routes based on a source protocol and autonomous system number, use the **match source-protocol** command in route-map configuration mode. To remove the protocol to be matched, use the **no** form of this command.

match source-protocol *source-protocol* [*autonomous-system-number*]

no match source-protocol *source-protocol* [*autonomous-system-number*]

Syntax Description

source-protocol	Protocol to match. The valid keywords are **bgp**, **connected**, **eigrp, isis**, **ospf**, **rip**, and **static**. There is no default.
autonomous-system-number	(Optional) Autonomous system number. This argument is not applicable to the **connected**, **rip**, and **static** keywords. The range is 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.

Command Default

EIGRP external routes are not matched on a source protocol and autonomous system number.

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
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.

Release	Modification
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.

Usage Guidelines

This command may not be useful with a redistribution operation that employs route maps because redistribution usually requires the configuration of a source protocol and an autonomous system value in order to redistribute. In many cases, it is more useful to configure a route map that includes matching the route type based on the source protocol and autonomous system using the **distribute-list** command for EIGRP.

Examples

The following example shows how to configure a route map to match a source protocol of BGP and an autonomous system 45000. When the match clause is true, the tag value of the destination routing protocol is set to 5. The route map is used to distribute incoming packets for an EIGRP process.

```
route-map metric_source
 match source-protocol bgp 45000
 set tag 5
!
router eigrp 1
 network 172.16.0.0
 distribute-list route-map metric_source in
```

The following example shows how to configure a route map to match a source protocol of BGP and a 4-byte autonomous system of 65538 in asplain format. When the match clause is true, the tag value of the destination routing protocol is set to 5. The route map is used to distribute incoming packets for an EIGRP process. 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.

```
route-map metric_source
 match source-protocol bgp 65538
 set tag 5
!
router eigrp 1
 network 172.16.0.0
 distribute-list route-map metric_source in
```

The following example shows how to configure a route map to match a source protocol of BGP and a 4-byte autonomous system of 1.2 in asdot format. When the match clause is true, the tag value of the destination routing protocol is set to 5. The route map is used to distribute incoming packets for an EIGRP process. This example requires Cisco IOS Release 12.0(32)S12, 12.4(24)T, or Cisco IOS XE

Release 2.3 where asdot notation is the only format for 4-byte autonomous system numbers. This configuration can also be performed using 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.

```
route-map metric_source
 match source-protocol bgp 1.2
 set tag 5
!
router eigrp 1
 network 172.16.0.0
 distribute-list route-map metric_source in
```

Related Commands

Command	Description
distribute-list	Filters networks received in updates.
match tag	Redistributes routes in the routing table that match the specified tags.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
router bgp	Configures the BGP routing process.
set as-path	Modifies an autonomous system path for BGP routes.
set tag (IP)	Sets a tag value of the destination routing protocol.

maximum-paths eibgp

To configure multipath load sharing for external Border Gateway Protocol (eBGP) and internal BGP (iBGP) routes, use the **maximum-paths eibgp** command in address family configuration mode. To disable multipath load sharing for eBGP and iBGP routes, use the **no** form of this command.

maximum-paths eibgp *number-of-paths* [**import** *number-of-import-paths*]

no maximum-paths eibgp *number-of-paths* [**import** *number-of-import-paths*]

Syntax Description

number-of-paths	Number of routes to install to the routing table. See the "Usage Guidelines" section for the number of paths that can be configured with this argument.
import *number-of-import-paths*	(Optional) Specifies the number of redundant paths that can be configured as back up multipaths for a virtual routing and forwarding (VRF) table. This keyword can be configured only under a VRF in address family configuration mode. **Note** We recommend that this keyword is enabled only where needed and that the number of import paths be kept to the minimum (typically, not more than two paths). For more information, see the related note in the "Usage Guidelines" section of this command page.

Command Default

BGP, by default, will install only one best path in the routing table.

Command Modes

Address family configuration (config-router-af)

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.0(24)S	This command was integrated into Cisco IOS Release 12.0(24)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.0(25)S	The **import** keyword was added.
12.3	The **import** keyword was added.
12.3(2)T	The maximum number of parallel routes was increased from 6 to 16.
12.2(25)S	The maximum number of parallel routes was increased from 6 to 16.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.0(1)M	This command was modified. The **import** keyword was replaced by the **import path selection** and **import path limit** commands.
12.2(33)SRE	This command was modified. The **import** keyword was replaced by the **import path selection** and **import path limit** commands.
Cisco IOS XE 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

The **maximum-paths eibgp** command is used to configure BGP multipath load sharing in a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) using eBGP and iBGP routes. This command is configured under a VRF in address family configuration mode. The number of multipaths is configured separately for each VRF.

The number of paths that can be configured is determined by the version of Cisco IOS software as shown in the following list:

- Cisco IOS Release 12.0S-based software: 8 paths
- Cisco IOS Release 12.3T, 12.4, 12.4T, and 15.0-based software: 16 paths
- Cisco IOS Release 12.2S-based software: 32 paths

The **maximum-paths eibgp** command cannot be configured with the **maximum-paths** or **maximum-paths ibgp** command because the **maximum-paths eibgp** command is a superset of these commands.

Note The configuration of this command does not override the existing outbound routing policy.

Configuring VRF Import Paths

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

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

The maximum number of import paths that can be configured in Cisco IOS Release 12.2SY-based software is 16.

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

In Cisco IOS Releases 15.0(1)M and 12.2(33)SRE, and in later releases, the **import** keyword was replaced by the **import path selection** and **import path limit** commands. If the **import** keyword is configured, the configuration is converted to the new commands, as show in the following example:

```
Router(config-router-af)# maximum-paths eibgp import 3
%NOTE: Import option has been deprecated.
%      Converting to 'import path selection all; import path limit 3'.
```

Examples

In the following example, the router is configured to install six eBGP or iBGP routes into the VRF routing table:

```
Router(config)# router bgp 40000
Router(config-router)# address-family ipv4 vrf vrf-1
Router(config-router-af)# maximum-paths eibgp 6
```

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

```
Router(config)# router bgp 45000
Router(config-router)# address-family ipv4 vrf vrf-2
Router(config-router-af)# maximum-paths eibgp 4 import 2
```

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

```
Router(config)# router bgp 50000
Router(config-router)# address-family ipv4 vrf vrf-3
Router(config-router-af)# maximum-paths eibgp import 2
```

Note Separate VRFs must be configured with different route distinguishers to support separate multipath configurations.

Related Commands

Command	Description
import path limit	Specifies the maximum number of BGP paths, per VRF importing net, that can be imported from an exporting net.
import path selection	Specifies the BGP import path selection policy for a specific VRF instance.
maximum-paths	Controls the maximum number of parallel routes an IP routing protocol can support.
maximum-paths ibgp	Configures the number of equal-cost or unequal-cost routes that BGP will install in the routing table.
show ip bgp	Displays entries in the BGP routing table.
show ip bgp vpnv4	Displays VPNv4 address information from the BGP table entries in the BGP routing table.

maximum-paths ibgp

To control the maximum number of parallel internal Border Gateway Protocol (iBGP) routes that can be installed in a routing table, use the **maximum-paths ibgp** command in router or address family configuration mode. To restore the default value, use the **no** form of this command.

Router Configuration Mode

maximum-paths ibgp *number-of-paths*

no maximum-paths ibgp *number-of-paths*

Under VRF in Address Family Configuration Mode

maximum-paths ibgp {*number-of-paths* [**import** *number-of-import-paths*] | **unequal-cost** *number-of-import-paths*}

no maximum-paths ibgp {*number-of-paths* [**import** *number-of-import-paths*] | **unequal-cost** *number-of-import-paths*}

Syntax Description

number-of-paths	Number of routes to install to the routing table. See the "Usage Guidelines" section for the number of paths that can be configured with this argument.
import *number-of-import-paths*	(Optional) Specifies the number of redundant paths that can be configured as backup multipaths for a virtual routing and forwarding (VRF) instance. This keyword can be configured only under a VRF in address family configuration mode. **Note** We recommend that this keyword is enabled only where needed and that the number of import paths be kept to the minimum (typically, not more than two paths). For more information, see the related note in the "Usage Guidelines" section of this command page.
unequal-cost *number-of-import-paths*	Specifies the number of unequal-cost routes to install in the routing table. See the "Usage Guidelines" section for the number of paths that can be configured. This keyword can be configured only under a VRF instance in address family configuration mode.

Command Default

BGP, by default, will install only one best path in the routing table.

Command Modes

Address family configuration (config-router-af)
Router configuration (config-router)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(25)S	The **import** keyword was added.

Release	Modification
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX.
12.3	The **import** keyword was added.
12.3(2)T	The maximum number of parallel routes was increased from 6 to 16.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S for use in IPv6.
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.
15.0(1)M	This command was modified. The **import** keyword was replaced by the **import path selection** and **import path limit** commands.
12.2(33)SRE	This command was modified. The **import** keyword was replaced by the **import path selection** and **import path limit** commands.
Cisco IOS XE 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

The **maximum-paths ibgp** command is used to configure equal-cost or unequal-cost multipath load sharing for iBGP peering sessions. In order for a route to be installed as a multipath in the BGP routing table, the route cannot have a next hop that is the same as another route that is already installed. The BGP routing process will still advertise a best path to iBGP peers when iBGP multipath load sharing is configured. For equal-cost routes, the path from the neighbor with the lowest router ID is advertised as the best path.

To configure BGP equal-cost multipath load sharing, all path attributes must be the same. The path attributes include weight, local preference, autonomous system path (entire attribute and not just the length), origin code, Multi Exit Discriminator (MED), and Interior Gateway Protocol (IGP) distance.

The number of paths that can be configured is determined by the version of Cisco IOS software as shown in the following list:

- Cisco IOS Release 12.0S-based software: 8 paths
- Cisco IOS Release 12.3T, 12.4, 12.4T, and 15.0-based software: 16 paths
- Cisco IOS Release 12.2S-based software: 32 paths

Note In IPv6, the **maximum-paths ibgp** command does not work for prefixes learned from iBGP neighbors that have been configured to distribute a Multiprotocol Label Switching (MPLS) label with its IPv6 prefix advertisements. If multiple routes exist for such prefixes, all of them are inserted into the Routing Information Base (RIB) when the **maximum-paths ibgp** command is configured, but only one is used and no load balancing occurs between equal-cost paths. The **maximum-paths ibgp** command works with 6PE only in Cisco IOS Release 12.2(25)S and subsequent 12.2S releases.

Configuring VRF Import Paths

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

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

The maximum number of import paths that can be configured in Cisco IOS Release 12.2SY-based software is 16.

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

In Cisco IOS Releases 15.0(1)M and 12.2(33)SRE, and in later releases, the **import** keyword was replaced by the **import path selection** and **import path limit** commands. If the **import** keyword is configured, the configuration is converted to the new commands, as show in the following example:

```
Router(config-router-af)# maximum-paths ibgp import 3
%NOTE: Import option has been deprecated.
%      Converting to 'import path selection all; import path limit 3'.
```

Examples

The following example configuration installs three parallel iBGP paths in a non-MPLS topology:

```
Router(config)# router bgp 100
Router(config-router)# maximum-paths ibgp 3
```

The following example configuration installs three parallel iBGP paths in an MPLS Virtual Private Network (VPN) topology:

```
Router(config)# router bgp 100
Router(config-router)# address-family ipv4 unicast vrf vrf-A
Router(config-route-af)# maximum-paths ibgp 3
```

The following example configuration installs two parallel routes in the VRF table:

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

The following example configuration installs two parallel routes in the VRF table:

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

Related Commands

Command	Description
import path limit	Specifies the maximum number of BGP paths, per VRF importing net, that can be imported from an exporting net.
import path selection	Specifies the BGP import path selection policy for a specific VRF instance.
maximum-paths	Controls the maximum number of parallel routes an IP routing protocol can support.
maximum-paths ibgp	Configures the number of equal-cost or unequal-cost routes that BGP will install in the routing table.
show ip bgp	Displays entries in the BGP routing table.
show ip bgp vpnv4	Displays VPNv4 address information from the BGP table entries in the BGP routing table.

neighbor activate

To enable the exchange of information with a Border Gateway Protocol (BGP) neighbor, use the **neighbor activate** command in address family configuration mode or router configuration mode. To disable the exchange of an address with a BGP neighbor, use the **no** form of this command.

neighbor {*ip-address* | *peer-group-name* | *ipv6-address***%**} **activate**

no neighbor {*ip-address* | *peer-group-name* | *ipv6-address***%**} **activate**

Syntax Description

ip-address	IP address of the neighboring router.
peer-group-name	Name of the BGP peer group.
ipv6-address	IPv6 address of the BGP neighbor.
%	(Optional) IPv6 link-local address identifier. This keyword needs to be added whenever a link-local IPv6 address is used outside the context of its interface.

Command Default

The exchange of addresses with BGP neighbors is enabled for the IPv4 address family. Enabling address exchange for all other address families is disabled.

Note Address exchange for address family IPv4 is enabled by default for each BGP routing session configured with the **neighbor remote-as** command unless you configure the **no bgp default ipv4-activate** command before configuring the **neighbor remote-as** command, or you disable address exchange for address family IPv4 with a specific neighbor by using the **no** form of the **neighbor activate** command.

Command Modes

Address family configuration
Router configuration

Command History

Release	Modification
11.0	This command was introduced.
12.0(5)T	Support for address family configuration mode and the IPv4 address family was added.
12.2(2)T	The *ipv6-address* argument and support for the IPv6 address family were 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.
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.
12.2(33)SRB	The **%** keyword was added

Release	Modification
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

Use this command to advertise address information in the form of an IP or IPv6 prefix. The address prefix information is known as Network Layer Reachability Information (NLRI) in BGP.

The **%** keyword is used whenever link-local IPv6 addresses are used outside the context of their interfaces. This keyword does not need to be used for non-link-local IPv6 addresses.

Examples

Address Exchange Example for Address Family vpn4

The following example shows how to enable address exchange for address family vpnv4 for all neighbors in the BGP peer group named PEPEER and for the neighbor 10.0.0.44:

```
Router(config)# address-family vpnv4
Router(config-router-af)# neighbor PEPEER activate
Router(config-router-af)# neighbor 10.0.0.44 activate
Router(config-router-af)# exit-address-family
```

Address Exchange Example for Address Family IPv4 Unicast

The following example shows how to enable address exchange for address family IPv4 unicast for all neighbors in the BGP peer group named group1 and for the BGP neighbor 172.16.1.1:

```
Router(config)# address-family ipv4 unicast
Router(config-router-af)# neighbor group1 activate
Router(config-router-af)# neighbor 172.16.1.1 activate
```

Address Exchange Example for Address Family IPv6

The following example shows how to enable address exchange for address family IPv6 for all neighbors in the BGP peer group named group2 and for the BGP neighbor 7000::2:

```
Router(config)# address-family ipv6
Router(config-router-af)# neighbor group2 activate
Router(config-router-af)# neighbor 7000::2 activate
```

Related Commands

Command	Description
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard IPv4 address prefixes.
address-family ipv6	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard IPv6 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard VPNv4 address prefixes.
address-family vpnv6	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard VPNv6 address prefixes.

exit-address-family	Exits from the address family submode.
neighbor remote-as	Adds an entry to the BGP or multiprotocol BGP neighbor table.

neighbor advertise best-external

To have a neighbor receive the advertisement of the best external path, use the **neighbor advertise best-external** command in address family configuration mode. To remove the designation, use the **no** form of the command.

neighbor {*ip-address* | *ipv6-address* | *peer-group-name* | *policy-template-name*} **advertise best-external**

no neighbor {*ip-address* | *ipv6-address* | *peer-group-name* | *policy-template-name*} **advertise best-external**

Syntax Description

ip-address	Advertises the best external path to this IPv4 neighbor.
ipv6-address	Advertises the best external path to this IPv6 neighbor.
peer-group-name	Advertises the best external path to this peer group.
policy-template-name	Advertises the best external path to neighbors described by the policy template.

Command Default

This command is disabled by default; the BGP bestpath is advertised to neighbors.

Command Modes

Address family configuration (config-router-af)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

Usage Guidelines

By default, the BGP bestpath is advertised to a peer. However, if the BGP Diverse Path feature is configured, you can use this command to specify that the best external path is advertised to the peer also.

This command does not enable the BGP Best External feature or the BGP Diverse Path feature. The **bgp additional-paths select best-external** command must be configured before the **neighbor advertise best-external** command can be configured. If the **neighbor advertise best-external** command is configured, but the **bgp additional-paths select best-external** command is not configured, an error message is generated.

This command can be configured for non-client iBGP peers only. It can be configured at the PE, ASBR, or RR. When it is configured at an RR, the best-external functionality is inter-cluster, best-external functionality.

When the **neighbor advertise best-external** command is configured:

- At the PE:
  - If the new style command (**bgp additional-paths select best-external**) is used to calculate the best external path, the best external path is advertised.

  - If the old style command (**bgp advertise-best-external**) command is already present, the **neighbor advertise best-external** command cannot be configured and an error message is generated.

- At the RR:
  - The RR advertises the best internal path to non-client iBGP peers only when the overall best path is a path learned from another cluster.

    This command cannot be configured on an RR toward its clients; it can be configured only for non-client RRs.

Examples

In the following example, the neighbor at 10.1.1.1 is configured to receive the advertisement of the best-external path:

```
router bgp 1
 neighbor 10.1.1.1 remote-as 1
 address-family ipv4 unicast
 neighbor 10.1.1.1 activate
 maximum-paths ibgp 4
 bgp bestpath igp-metric ignore
 bgp additional-paths select best-external
 bgp additional-paths install
 neighbor 10.1.1.1 advertise best-external
```

Related Commands

Command	Description
bgp additional-paths select best-external	Specifies that the system compute a second BGP bestpath among those received from external neighbors.
bgp advertise-best-external	Enables BGP to calculate an external route as the best backup path for a given address family, to install it into the RIB and Cisco Express Forwarding, and to advertise the best external path to its neighbors.
bgp bestpath igp-metric ignore	Specifies that the system ignore the IGP metric during best path selection.
maximum-paths ebgp	Configures multipath load sharing for eBGP and iBGP routes.
maximum-paths ibgp	Controls the maximum number of parallel iBGP routes that can be installed in a routing table.

neighbor advertise diverse-path

To specify that an additional path (a backup path or multipath or both) is advertised to a peer in addition to the bestpath, use the **neighbor advertise diverse-path** command in address family configuration mode. To remove the designation, use the **no** form of the command.

neighbor {*ip-address* | *ipv6-address* | *peer-group-name* | *policy-template-name*} **advertise diverse-path** {**backup** [**mpath**] | **mpath**}

no neighbor {*ip-address* | *ipv6-address* | *peer-group-name* | *policy-template-name*} **advertise diverse-path** {**backup** [**mpath**] | **mpath**}

Syntax Description

ip-address	Advertises a diverse path to this IPv4 neighbor.
ipv6-address	Advertises a diverse path to this IPv6 neighbor.
peer-group-name	Advertises a diverse path to this peer group.
policy-template-name	Advertises a diverse path to neighbors described by the policy template?
backup	(Optional) Advertises the backup path. If **backup** is specifed, but there is no backup path, the best path is advertised.
mpath	(Optional) Advertises the multipath, which is the second best path. If **mpath** is specifed, but there is no multipath, the best path is advertised. If both **backup** and **mpath** are specified, the multipath is advertised.

Command Default

This command is disabled by default; the BGP bestpath is advertised to neighbors.

Command Modes

Address family configuration (config-router-af)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

Usage Guidelines

By default, the BGP bestpath is advertised to a peer. However, if the BGP Diverse Path feature is configured, you can use this command to specify that the backup path or multipath (or both) is advertised to the peer also. This command is not supported for VRFs.

This command does not enable the BGP Diverse Path feature. If this command is configured, but the BGP Diverse Path feature is not configured (by one of the commands in the Related Commands table), a warning message is generated.

If any of the Related Commands is configured, but there is no multipath or backup path (no additional path), then the specified neighbor will receive the bestpath in advertisements.

Neighbors for which this command is not specified will receive the bestpath in advertisements.

This command can be configured for route reflector clients only (because the BGP Diverse Path feature applies within an AS and within a single cluster).

If the **bgp additional-paths select backup** command was configured and is subsequently removed from the configuration before the **neighbor advertise diverse-path backup** command is removed, then the specified neighbor will receive the bestpath in advertisements.

Note If the old style command for BGP PIC or Best External is already configured (**bgp additional-paths install** or **bgp advertise-best-external**), the **neighbor advertise diverse-path** command cannot be configured; an error message is generated.

Either the **backup** keyword or the **mpath** keyword is required; both keywords can be specified.

Examples

In the following example, the neighbor at 10.1.1.1 will receive an advertisement for a backup path in addition to the bestpath:

```
router bgp 1
 neighbor 10.1.1.1 remote-as 1
 address-family ipv4 unicast
 neighbor 10.1.1.1 activate
 maximum-paths ibgp 4
 bgp bestpath igp-metric ignore
 bgp additional-paths select backup
 bgp additional-paths install
neighbor 10.1.1.1 advertise diverse-path backup
```

Related Commands

Command	Description
bgp additional-paths install	Enables BGP to calculate a backup path for a given address and to install it into the RIB and CEF.
bgp additional-paths select backup	Specifies that the system compute a second BGP bestpath as a backup path.
maximum-paths ebgp	Configures multipath load sharing for eBGP and iBGP routes.
maximum-paths ibgp	Controls the maximum number of parallel iBGP routes that can be installed in a routing table.

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.
advertise-map *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.
exist-map *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.
non-exist-map *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

Router configuration

Command History

Release	Modification
11.1CC	This command was introduced.
11.2	This command was integrated into Cisco IOS Release 11.2.
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 **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 nonexist map. If the condition is not met, the route is withdrawn and conditional advertisement does not occur. All routes that may be dynamically advertised or not advertised need to exist in the BGP routing table for conditional advertisement to occur.

Examples

The following 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 5
 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 nonexist map. If the prefix exists in MAP3 but not MAP4, the condition is met and the prefix is advertised.

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

Related Commands

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

neighbor advertisement-interval

To set the minimum route advertisement interval (MRAI) between the sending of BGP routing updates, use the **neighbor advertisement-interval** command in address family or router configuration mode. To restore the default value, 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

ip-address	IP address of the neighbor.
peer-group-name	Name of a BGP peer group.
seconds	Time (in seconds) is specified by an integer ranging from 0 to 600.

Defaults

eBGP sessions not in a VRF: 30 seconds
eBGP sessions in a VRF: 0 seconds
iBGP sessions: 0 seconds

Command Modes

Router configuration

Command History

Release	Modification
10.3	This command was introduced.
12.0(7)T	Address family configuration mode 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.
12.4T, 12.2SB, 12.2SE, 12.2SG, 12.2SR, 12.2SX, Cisco IOS XE 2.1	This command was modified. The default value for eBGP sessions in a VRF and for iBGP sessions changed from .5 seconds to 0 seconds.

Usage Guidelines

When the MRAI is equal to 0 seconds, BGP routing updates are sent as soon as the BGP routing table changes.

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

Examples

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

```
router bgp 5
 neighbor 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 5
address-family ipv4 unicast
 neighbor 10.4.4.4 advertisement-interval 10
```

Related Commands

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

neighbor capability orf prefix-list

To advertise outbound route filter (ORF) capabilities to a peer router, use the **neighbor capability orf prefix-list** 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-list** [**receive** | **send** | **both**]

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

Syntax Description

ip-address	The IP address of the neighbor router.
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.

Command Default

No ORF capabilities are advertised to a peer router.

Command Modes

Address family

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.
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.
12.2(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 **neighbor capability orf prefix-list** 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 examples configure routers to advertise ORF send or receive capabilities to BGP neighbors.

Router-A Configuration (Sender)

The following example creates an outbound route filter and configures Router-A (10.1.1.1) to advertise the filter to Router-B (172.16.1.2). An IP prefix list named FILTER is created to specify the 192.168.1.0/24 subnet for outbound route filtering. The ORF send capability is configured on Router-A so that Router-A can advertise the outbound route filter to Router-B.

```
ip prefix-list FILTER seq 10 permit 192.168.1.0/24
!
router bgp 100
 address-family ipv4 unicast
 neighbor 172.16.1.2 remote-as 200
 neighbor 172.16.1.2 ebgp-multihop
 neighbor 172.16.1.2 capability orf prefix-list send
 neighbor 172.16.1.2 prefix-list FILTER in
 exit
```

Router-B Configuration (Receiver)

The following example configures Router-B to advertise the ORF receive capability to Router-A. Router-B will install the outbound route filter, defined in the FILTER prefix list, after ORF capabilities have been exchanged. An inbound soft reset is initiated on Router-B at the end of this configuration to activate the outbound route filter.

```
router bgp 200
 address-family ipv4 unicast
 neighbor 10.1.1.1 remote-as 100
 neighbor 10.1.1.1 ebgp-multihop 255
 neighbor 10.1.1.1 capability orf prefix-list receive
 end
clear ip bgp 10.1.1.1 in prefix-filter
```

Note The inbound soft refresh must be initiated with the **clear ip bgp** command in order for the BGP ORF feature to function.

Related Commands

Command	Description
neighbor prefix-list	Distributes BGP neighbor information as specified in a prefix list.

neighbor default-originate

To allow a BGP speaker (the local router) to send the default route 0.0.0.0 to a neighbor for use as a default route, use the **neighbor default-originate** 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

ip-address	IP address of the neighbor.
peer-group-name	Name of a BGP peer group.
route-map *map-name*	(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.
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

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

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

Examples

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

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

In the following example, the local router injects route 0.0.0.0 to the neighbor 172.16.2.3 only if there is a route to 192.168.68.0 (that is, if a route with any mask exists, such as 255.255.255.0 or 255.255.0.0):

```
router bgp 109
 network 172.16.0.0
 neighbor 172.16.2.3 remote-as 200
 neighbor 172.16.2.3 default-originate route-map default-map
!
route-map default-map 10 permit
 match ip address 1
!
access-list 1 permit 192.168.68.0
```

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 192.168.68.0 with a mask of 255.255.0.0:

```
router bgp 109
 network 172.16.0.0
 neighbor 172.16.2.3 remote-as 200
 neighbor 172.16.2.3 default-originate route-map default-map
!
route-map default-map 10 permit
 match ip address 100
!
access-list 100 permit ip host 192.168.68.0 host 255.255.0.0
```

Related Commands

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

neighbor description

To associate a description with a neighbor, use the **neighbor description** command in router configuration mode or address family 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

ip-address	IP address of the neighbor.
peer-group-name	Name of an EIGRP peer group. This argument is not available in address-family configuration mode.
text	Text (up to 80 characters in length) that describes the neighbor.

Command Default

There is no description of the neighbor.

Command Modes

Router configuration (config-router)
Address family configuration (config-router-af)

Command History

Release	Modification
11.3	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.
15.0(1)M	This command was modified. Address-family configuration mode was added.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Examples

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

```
Router(config)# router bgp 109
Router(config-router)# network 172.16.0.0
Router(config-router)# neighbor 172.16.2.3 description peer with example.com
```

In the following example, the description of the address family neighbor is “address-family-peer”:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# network 172.16.0.0
Router(config-router-af)# neighbor 172.16.2.3 description address-family-peer
```

Related Commands

Command	Description
address-family (EIGRP)	Enters address family configuration mode to configure an EIGRP routing instance.
network (EIGRP)	Specifies the network for an EIGRP routing process.
router eigrp	Configures the EIGRP address family process.

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

ip-address	IP address of a neighbor.
peer-group-name	Name of a BGP peer group.

Command Default

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
neighbor ebgp-multihop	Accepts or initiates BGP connections to external peers residing on networks that are not directly connected.
neighbor update-source	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

ip-address	IP address of the neighbor.
peer-group-name	Name of a BGP peer group.
access-list-number	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.
access-list-name	Name of a standard or extended access list.
prefix-list-name	Name of a BGP prefix list.
in	Access list is applied to incoming advertisements to that neighbor.
out	Access list is applied to outgoing advertisements to that neighbor.

Defaults

No BGP neighbor is specified.

Command Modes

Address family
Router configuration

Command History

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

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 neighbor172.16.4.1. List 39 permits the advertisement of network 10.109.0.0.

```
router bgp 109
 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 109
 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
access-list (IP extended)	Defines an extended IP access list.
access-list (IP standard)	Defines a standard IP access list.
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
ip as-path access-list	Defines a BGP-related access list.
neighbor filter-list	Sets up a BGP filter.
neighbor peer-group (creating)	Creates a BGP peer group.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another.

neighbor dmzlink-bw

To configure Border Gateway Protocol (BGP) 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 link bandwidth advertisement, use the **no** form of this command.

neighbor *ip-address* **dmzlink-bw**

no neighbor *ip-address* **dmzlink-bw**

Syntax Description

ip-address	IP address of the neighbor router for which the bandwidth of the outbound link is advertised.

Command Default

This command is disabled by default.

Command Modes

Address family configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.0(24)S	This command was integrated into Cisco IOS Release 12.0(24)S.
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 **neighbor dmzlink-bw** command is used to configure BGP to advertise the bandwidth of the specified external interface as an extended community. This command is configured for links between directly connected external BGP (eBGP) neighbors. The link bandwidth extended community attribute is propagated to iBGP peers when extended community exchange is enabled with the **neighbor send-community** command. This feature is used with BGP multipath features to configure load balancing over links with unequal bandwidth. This feature is not enabled until the **bgp dmzlink-bw** command is entered under the address family session for each router that has a directly connected external link.

Examples

In the following example, the BGP Link Bandwidth feature is configured to allow multipath load balancing to distribute link traffic proportionally to the bandwidth of each external link, and to advertise the bandwidth of these links to iBGP peers as an extended community:

```
Router(config)# router bgp 100
Router(config-router)# neighbor 10.10.10.1 remote-as 100
Router(config-router)# neighbor 10.10.10.1 update-source Loopback 0
Router(config-router)# neighbor 10.10.10.3 remote-as 100
```

```
Router(config-router)# neighbor 10.10.10.3 update-source Loopback 0
Router(config-router)# neighbor 172.16.1.1 remote-as 200
Router(config-router)# neighbor 172.16.1.1 ebgp-multihop 1
Router(config-router)# neighbor 172.16.2.2 remote-as 200
Router(config-router)# neighbor 172.16.2.2 ebgp-multihop 1
Router(config-router)# address-family ipv4
Router(config-router-af)# bgp dmzlink-bw
Router(config-router-af)# neighbor 10.10.10.1 activate
Router(config-router-af)# neighbor 10.10.10.1 next-hop-self
Router(config-router-af)# neighbor 10.10.10.1 send-community both
Router(config-router-af)# neighbor 10.10.10.3 activate
Router(config-router-af)# neighbor 10.10.10.3 next-hop-self
Router(config-router-af)# neighbor 10.10.10.3 send-community both
Router(config-router-af)# neighbor 172.16.1.1 activate
Router(config-router-af)# neighbor 172.16.1.1 dmzlink-bw
Router(config-router-af)# neighbor 172.16.2.2 activate
Router(config-router-af)# neighbor 172.16.2.2 dmzlink-bw
Router(config-router-af)# maximum-paths ibgp 6
Router(config-router-af)# maximum-paths 6
```

Related Commands

Command	Description
bgp dmzlink-bw	Configures BGP to distribute traffic proportionally over external links with unequal bandwidth when multipath load balancing is enabled.
neighbor send-community	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* | *ipv6-address* | *peer-group-name*} **ebgp-multihop** [*ttl*]

no neighbor {*ip-address* | *ipv6-address* | *peer-group-name*} **ebgp-multihop**

Syntax Description

ip-address	IP address of the BGP-speaking neighbor.
ipv6-address	IPv6 address of the BGP-speaking neighbor.
peer-group-name	Name of a BGP peer group.
ttl	(Optional) Time-to-live in the range from 1 to 255 hops.

Command Default

Only directly connected neighbors are allowed.

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
11.0	The *peer-group-name* argument was added.
12.2(33)SRA	The *ipv6-address* argument and support for the IPv6 address family were added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

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

neighbor fall-over

To enable Border Gateway Protocol (BGP) to monitor the peering session of a specified neighbor for adjacency changes and to deactivate the peering session, use the **neighbor fall-over** command in address family or router configuration mode. To disable BGP monitoring of the neighbor peering session, use the **no** form of this command.

neighbor {*ip-address* | *ipv6-address*} **fall-over** [**bfd** | **route-map** *map-name*]

no neighbor {*ip-address* | *ipv6-address*} **fall-over** [**bfd** | **route-map** *map-name*]

Syntax Description

ip-address	IPv4 address of a BGP neighbor.
ipv6-address	IPv6 address of a BGP neighbor.
bfd	(Optional) Enables Bidirectional Forwarding Detection (BFD) protocol support for fallover.
route-map *map-name*	(Optional) Specifies the use of a route map by name.  **Note** The route map applies only to a neighbor with an IPv4 address.

Command Default

BGP does not monitor neighbor peering sessions.

Command Modes

Address family configuration (config-router-af)
Router configuration (config-router)

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.
12.4(4)T	The **route-map** keyword and *map-name* argument were added to support the BGP Selective Address Tracking feature.
12.2(33)SRA	The **bfd** keyword was added to support the BFD feature, and this command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	The **route-map** keyword and *map-name* argument were added to support the BGP Selective Address Tracking feature.
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.
12.2(33)SB	The **bfd** keyword was added to support the BFD feature, and this command was integrated into Cisco IOS Release 12.2(33)SB.
15.1(2)S	This command was modified. The *ipv6-address* argument was added.
Cisco IOS XE 3.3S	This command was modified. The *ipv6-address* argument was added.

Usage Guidelines

The **neighbor fall-over** command is a BGP neighbor session command that is used to enable BGP fast peering session deactivation. BGP fast peering session deactivation improves BGP convergence and response time to adjacency changes with BGP neighbors. BGP fast peering session deactivation is event-driven and is configured on a per-neighbor basis. When BGP fast peering session deactivation 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.

In Cisco IOS Release 12.4(4)T, 12.2(33)SRB, and later releases, the optional **route-map** keyword and *map-name* argument are used with this command to determine if a peering session with a BGP neighbor should be deactivated (reset) when a route to the BGP peer changes. The route map is evaluated against the new route, and if a deny statement is returned, the peer session is reset. The route map is not used for session establishment.

Note Only the **match ip address** and **match source-protocol** commands are supported in the route map. No **set** commands or other **match** commands are supported.

In Cisco IOS Release 12.2(33)SRA, 12.2(33)SB, and later releases, the optional **bfd** keyword is used to enable BFD protocol support for fallover. BFD provides fast forwarding path failure detection and a consistent failure detection method for network administrators. Because the network administrator can use BFD to detect forwarding path failures at a uniform rate, rather than the variable rates for different routing protocol hello mechanisms, network profiling and planning will be easier, and reconvergence time will be consistent and predictable. The main benefit of implementing BFD for BGP is a marked decrease in reconvergence time.

In Cisco IOS Release 15.1(2)S, Cisco IOS XE Release 3.3S, and later releases, an IPv6 address can be specified with the **bfd** keyword. Once it has been verified that BFD neighbors are up, the **show bgp ipv6 unicast neighbors** command with a specified IPv6 address will display that BFD is being used to detect fast fallover.

Examples

In the following example, the BGP routing process is configured to monitor and use fast peering session deactivation for the neighbor session with the neighbor at 192.168.1.2:

```
router bgp 45000
 neighbor 192.168.1.2 remote-as 40000
 neighbor 192.168.1.2 fall-over
 end
```

In the following example, the BGP peering session will be reset if a route with a prefix of /28 or a more specific route to a peer destination is no longer available:

```
router bgp 45000
 neighbor 192.168.1.2 remote-as 40000
 neighbor 192.168.1.2 fall-over route-map CHECK-NBR
 exit
ip prefix-list FILTER28 seq 5 permit 0.0.0.0/0 ge 28
route-map CHECK-NBR permit 10
 match ip address prefix-list FILTER28
 end
```

In the following example, BFD is enabled for Fast Ethernet interface 0/1 with a specified BFD interval. The BGP peering session is also BFD enabled and this will result in a decreased reconvergence time for BGP if any of the forwarding paths to specified neighbors fail.

```
interface FastEthernet 0/1
 ip address 172.16.10.1 255.255.255.0
```

```
 bfd interval 50 min_rx 50 multiplier 3
 exit
router bgp 40000
 bgp log-neighbor-changes
 neighbor 172.16.10.2 remote-as 45000
 neighbor 172.16.10.2 fall-over bfd
 exit
```

In the following IPv6 example, BFD is enabled for Fast Ethernet interface 0/1 with a specified BFD interval. The BGP peering session is also BFD enabled and this will result in a decreased reconvergence time for BGP if any of the forwarding paths to the specified neighbor at 2001:DB8:2:1::4 fail.

```
ipv6 unicast-routing
ipv6 cef
interface fastethernet 0/1
 ipv6 address 2001:DB8:1:1::1/64
 bfd interval 500 min_rx 500 multiplier 3
 no shutdown
 exit
router bgp 65000
 no bgp default ipv4-unicast
 address-family ipv6 unicast
 bgp log-neighbor-changes
 neighbor 2001:DB8:2:1::4 remote-as 45000
 neighbor 2001:DB8:2:1::4 fall-over bfd
 end
```

Related Commands

Command	Description
bfd	Sets the baseline BFD session parameters on an interface.
match ip address	Matches IP addresses defined by a prefix list.
match source-protocol	Matches the route type based on the source protocol.
show bgp ipv6 unicast neighbors	Displays information about BGP IPv6 neighbors.

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

ip-address	IP address of the neighbor.
peer-group-name	Name of a BGP peer group.
access-list-number	Number of an autonomous system path access list. You define this access list with the **ip as-path access-list** command.
in	Access list is applied to incoming routes.
out	Access list is applied to outgoing routes.

Command Default

No BGP filter is used.

Command Modes

Router configuration or Address family configuration

Command History

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

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

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.

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

In the following router configuration mode example, the BGP neighbor with IP address 172.16.1.1 is not sent advertisements about any path through or from the adjacent autonomous system 123:

```
ip as-path access-list 1 deny _123_
ip as-path access-list 1 deny ^123$

 router bgp 109
 network 10.108.0.0
 neighbor 192.168.6.6 remote-as 123
 neighbor 172.16.1.1 remote-as 47
 neighbor 172.16.1.1 filter-list 1 out
```

In the following address family configuration mode example, the BGP neighbor with IP address 172.16.1.1 is not sent advertisements about any path through or from the adjacent autonomous system 123:

```
ip as-path access-list 1 deny _123_
ip as-path access-list 1 deny ^123$

router bgp 109
 address-family ipv4 unicast
  network 10.108.0.0
  neighbor 192.168.6.6 remote-as 123
  neighbor 172.16.1.1 remote-as 47
  neighbor 172.16.1.1 filter-list 1 out
```

Related Commands

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

neighbor ha-mode graceful-restart

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

neighbor {*ip-address* | *peer-group-name*} **ha-mode graceful-restart** [**disable**]

no neighbor {*ip-address* | *peer-group-name*} **ha-mode graceful-restart** [**disable**]

Syntax Description

ip-address	IP address of the neighbor.
peer-group-name	Name of a BGP peer group.
disable	(Optional) Disables BGP graceful restart capability for a neighbor.

Command Default

BGP graceful restart capability is disabled.

Command Modes

Router configuration (config-router)

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.

Usage Guidelines

The **neighbor ha-mode graceful-restart** command is used to enable or disable the graceful restart capability for an individual BGP neighbor or peer group in a BGP network. 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.

To enable the BGP graceful restart capability globally for all BGP neighbors, use the **bgp graceful-restart** command. When the BGP graceful restart capability is configured for an individual neighbor, each method of configuring graceful restart has the same priority, and the last configuration instance is applied to the neighbor.

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 neighbor, 172.21.1.2:

```
router bgp 45000
 bgp log-neighbor-changes
 address-family ipv4 unicast
 neighbor 172.21.1.2 remote-as 45000
 neighbor 172.21.1.2 activate
 neighbor 172.21.1.2 ha-mode graceful-restart
 end
```

The following example enables the BGP graceful restart capability globally for all BGP neighbors and then disables the BGP graceful restart capability for the BGP peer group PG1. The BGP neighbor 172.16.1.2 is configured as a member of the peer group PG1 and inherits the disabling of the BGP graceful restart capability.

```
router bgp 45000
 bgp log-neighbor-changes
 bgp graceful-restart
 address-family ipv4 unicast
 neighbor PG1 peer-group
 neighbor PG1 remote-as 45000
 neighbor PG1 ha-mode graceful-restart disable
 neighbor 172.16.1.2 peer-group PG1
 end
```

Related Commands

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

neighbor ha-mode sso

To configure a Border Gateway Protocol (BGP) neighbor to support BGP nonstop routing (NSR) with stateful switchover (SSO), use the **neighbor ha-mode sso** command in the appropriate command mode. To remove the configuration, use the **no** form of this command.

neighbor *ip-address* **ha-mode sso**

no neighbor *ip-address* **ha-mode sso**

Syntax Description

ip-address	IP address of the neighboring router.

Command Default

BGP NSR with SSO support is disabled.

Command Modes

Address family configuration
Session-template configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.
Cisco IOS XE 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

The **neighbor ha-mode sso** command is used to configure a BGP neighbor to support BGP NSR with SSO. BGP NSR with SSO is disabled by default.

BGP NSR with SSO is supported in BGP peer, BGP peer group, and BGP session template configurations. To configure BGP NSR with SSO in BGP peer and BGP peer group configurations, use the **neighbor ha-mode sso** command in address family configuration mode for IPv4 VRF address family BGP peer sessions. To include support for Cisco BGP NSR with SSO in a peer session template, use the **ha-mode sso** command in session-template configuration mode.

Examples

The following example shows how to configure a BGP neighbor to support SSO:

```
Router(config-router-af)# neighbor 10.3.32.154 ha-mode sso
```

Related Commands

Command	Description
show ip bgp vpnv4	Displays VPN address information from the BGP table.
show ip bgp vpnv4 all sso summary	Displays the number of BGP neighbors that support SSO.

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

ip-address	IP address of the neighbor.
policy-template-name	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.
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.

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

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

ip-address	IP address of the neighbor.
session-template-name	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.
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.

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
exit peer-session	Exits session-template configuration mode and enters router configuration mode.
inherit peer-session	Configures a peer session template to inherit the configuration from another peer session template.
show ip bgp neighbors	Displays information about the TCP and BGP connections to neighbors.
show ip bgp template peer-session	Displays locally configured peer session templates.
template peer-session	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* | *peer-group-name*} **local-as** [*autonomous-system-number* [**no-prepend** [**replace-as** [**dual-as**]]]]

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

Syntax Description

ip-address	IP address of the eBGP neighbor.
peer-group-name	Name of a BGP peer group.
autonomous-system-number	(Optional) Number of an autonomous system to prepend to the AS_PATH attribute. The range of values for this argument is any valid autonomous system number 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. **Note** With this argument, you cannot specify the autonomous system number from the local BGP routing process or from the network of the remote peer.
no-prepend	(Optional) Does not prepend the local autonomous system number to any routes received from the eBGP neighbor.
replace-as	(Optional) Replaces the real autonomous system number with the local autonomous system number in the eBGP updates. The autonomous system number from the local BGP routing process is not prepended.
dual-as	(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 *autonomous-system-number* argument (local-as).

Command Default

The autonomous system number from the local BGP routing process is prepended to all external routes by default.

Command Modes

Address family configuration (config-router-af)
Router configuration (config-router)

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.
12.2(8)T	The **no-prepend** keyword was added.
12.2(14)S	The **no-prepend** keyword was integrated into Cisco IOS Release 12.2(14)S.
12.0(18)S	The **no-prepend** keyword was integrated into Cisco IOS Release 12.0(18)S.
12.0(27)S	The **replace-as** and **dual-as** keywords were added.
12.2(25)S	The **replace-as** and **dual-as** keywords were integrated into Cisco IOS Release 12.2(25)S.
12.3(11)T	The **replace-as** and **dual-as** keywords were integrated into Cisco IOS Release 12.3(11)T.
12.2(27)SBC	This command was integrated into 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(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
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.
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.

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.

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 followed by the **clear ip bgp *** command to perform a hard reset of all current BGP sessions.

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.

To ensure a smooth transition, we recommend that all BGP speakers within an autonomous system that is identified using a 4-byte autonomous system number, be upgraded to support 4-byte autonomous system numbers.

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 Keyword 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 Keyword 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 Keyword 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
```

4-Byte Autonomous System Number no-prepend Keyword Configuration: Examples

The following example configures BGP to not prepend the 4-byte autonomous system number of 65536 in asplain format to routes received from the 192.168.1.2 neighbor. 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 bgp 65538
 address-family ipv4 multicast
  network 192.168.0.0
  neighbor 192.168.1.2 local-as 65536 no-prepend
```

The following example configures BGP to not prepend the 4-byte autonomous system number of 1.0 in asdot format to routes received from the 192.168.1.2 neighbor. 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, or Cisco IOS XE Release 2.3.

```
router bgp 1.2
 address-family ipv4 multicast
  network 192.168.0.0
  neighbor 192.168.1.2 local-as 1.0 no-prepend
```

Related Commands

Command	Description
bgp asnotation dot	Changes the default display and the regular expression match format of BGP 4-byte autonomous system numbers from asplain (decimal values) to dot notation.
neighbor remove-private-as	Removes private autonomous system numbers from outbound routing 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 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*] [**warning-only**]

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

Syntax Description

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

Defaults

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

Command Modes

Router configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

neighbor maximum-prefix (BGP)

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

ip-address	IP address of the neighbor.
peer-group-name	Name of a Border Gateway Protocol (BGP) peer group.
maximum	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.
threshold	(Optional) Integer specifying at what percentage of the *maximum*-prefix 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 *restart-interval* argument.
restart-interval	(Optional) Time interval (in minutes) that a peering session is reestablished. The range is from 1 to 65535 minutes.
warning-only	(optional) Allows the router to generate a sys-log message when the *maximum-prefix limit* is exceeded, instead of terminating the peering session.

Defaults

This command is disabled by default. Peering sessions are disabled when the maximum number of prefixes is exceeded. If the *restart-interval* argument is not configured, a disabled session will stay down after the maximum-prefix limit is exceeded.

threshold: 75 percent

Command Modes

Router configuration

Command History

Release	Modification
11.3	This command was introduced.
12.0(22)S	The **restart** keyword was introduced.
12.2(15)T	The **restart** keyword was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	The **restart** keyword was integrated into Cisco IOS Release 12.2(18)S.

Release	Modification
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.

Usage Guidelines

The **neighbor maximum-prefix** command allows you to configure a maximum number of prefixes that a Border Gateway Protocol (BGP) routing process will accept from the specified peer. This feature provides a 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, BGP disables the peering session (by default). If the **restart** keyword is configured, BGP will automatically reestablish the peering session at the configured time interval. If the **restart** keyword is not configured and a peering session is terminated because the maximum prefix limit has been exceed, the peering session will not be be reestablished until the **clear ip bgp** command is entered. If the **warning-only** keyword is configured, BGP sends only a log message and continues to peer with the sender.

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.

Examples

In the following example, the maximum prefixes that will be accepted from the 192.168.1.1 neighbor is set to 1000:

```
Router(config)# router bgp 40000
Router(config-router)# network 192.168.0.0
Router(config-router)# neighbor 192.168.1.1 maximum-prefix 1000
```

In the following example, the maximum number of prefixes that will be accepted from the 192.168.2.2 neighbor is set to 5000. The router is also configured to display warning messages when 50 percent of the maximum-prefix limit (2500 prefixes) has been reached.

```
Router(config)# router bgp 40000
Router(config-router)# network 192.168.0.0
Router(config-router)# neighbor 192.168.2.2 maximum-prefix 5000 50
```

In the following example, the maximum number of prefixes that will be accepted from the 192.168.3.3 neighbor is set to 2000. The router is also configured to reestablish a disabled peering session after 30 minutes.

```
Router(config)# router bgp 40000
Router(config-router) network 192.168.0.0
Router(config-router)# neighbor 192.168.3.3 maximum-prefix 2000 restart 30
```

In the following example, warning messages will be displayed when the threshold of the maximum-prefix limit (500 x 0.75 = 375) for the 192.168.4.4 neighbor is exceeded:

```
Router(config)# router bgp 40000
Router(config-router)# network 192.168.0.0
Router(config-router)# neighbor 192.168.4.4 maximum-prefix 500 warning-only
```

Related Commands

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

neighbor next-hop-self

To configure the router as the next hop for a BGP-speaking neighbor or peer group, use the **neighbor next-hop-self** command in router configuration mode. To disable this feature, use the **no** form of this command.

neighbor {*ip-address* | *peer-group-name*} **next-hop-self**

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

Syntax Description

ip-address	IP address of the BGP-speaking neighbor.
peer-group-name	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 *peer-group-name* argument 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

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

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

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

Examples

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

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

Related Commands

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

neighbor next-hop-unchanged

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

neighbor {*ip-address* | *ipv6-address* | *peer-group-name*} **next-hop-unchanged** [**allpaths**]

no neighbor {*ip-address* | *ipv6-address* | *peer-group-name*} **next-hop-unchanged** [**allpaths**]

Syntax Description

ip-address	Propagate the iBGP path's next hop unchanged for this IPv4 neighbor.
ipv6-address	Propagate the iBGP path's next hop unchanged for this IPv6 neighbor.
peer-group-name	Propagate the iBGP path's next hop unchanged for this BGP peer group.
allpaths	(Optional) Propagate the next hop unchanged, for all paths (iBGP and eBGP) to this neighbor.

Command Default

This command is disabled by default.

Command Modes

Address family configuration (config-router-af)
Router configuration (config-router)

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	The **allpaths** keyword was added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

By default, for eBGP, the next hop to reach a connected network is the IP address of the neighbor that sent the update. Therefore, as an update goes from router to router, the next hop typically changes to be the address of the neighbor that sent the update (the router's own address).

However, there might be a scenario where you want the next hop to remain unchanged. The **neighbor next-hop-unchanged** command is used to propagate the next hop unchanged for multihop eBGP peering sessions. This command is configured on an eBGP neighbor, but the neighbor propagates routes learned from iBGP;that is, the neighbor propagates the next hop of iBGP routes toward eBGP.

Caution Using the **neighbor next-hop-unchanged** command or incorrectly altering the BGP next hop can cause inconsistent routing, routing loops, or a loss of connectivity. It should only be attempted by someone who has a good understanding of the design implications.

This command can be used to configure MPLS VPNs between service providers by not modifying the next hop attribute when advertising routes to an eBGP peer.

Examples

The following example configures a multihop eBGP peer at 10.0.0.100 in a remote AS. When the local router sends updates to that peer, it will send them without modifying the next hop attribute.

```
router bgp 65535
 address-family ipv4
 neighbor 10.0.0.100 remote-as 65600
 neighbor 10.0.0.100 activate
 neighbor 10.0.0.100 ebgp-multihop 255
 neighbor 10.0.0.100 next-hop-unchanged
 end
```

Related Commands

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

neighbor password

To enable message digest5 (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

ip-address	IP address of the BGP-speaking neighbor.
peer-group-name	Name of a BGP peer group.
string	Case-sensitive password of up to 25 characters in length. The first character cannot be a number. The string can contain any alphanumeric characters, including spaces. You cannot specify a password in the format *number-space-anything*. The space after the number can cause authentication to fail.

Command Default

MD5 is not authenticated on a TCP connection between two BGP peers.

Command Modes

Router configuration (config-router)#

Command History

Release	Modification
11.0	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.
12.4(24)T	This command was integrated into Cisco IOS Release 12.2(24)T. The password was restricted to 25 characters regardless of whether the s**ervice password-encryption** command was enabled.

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 you can provide a case-sensitive password of up to 25 characters regardless of whether the **service password-encryption** command is enabled . If the length of password is more than 25 characters, an error message is displayed and the password is not accepted. 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 hold-down timer expires. The default time period is 180 seconds. If the password is not entered or changed on the remote router before the hold-down timer expires, the session will time out.

Note Configuring a new timer value for the hold-down timer will only take effect after the session has been reset. So, it is not possible to change the configuration of the hold-down 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 hold-down timer expires.

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

The following example configures a password for more than 25 characters when the **service password-encryption** command is disabled.

```
Router(config)# router bgp 200
Router(config-router)# bgp router-id 2.2.2.2
Router(config-router)# neighbor remote-as 3
Router(config-router)# neighbor 209.165.200.225 password 12345678912345678912345678901
% BGP: Password length must be less than or equal to 25.

Router(config-router)# do show run | i password
no service password-encryption
 neighbor 209.165.200.225 password 123456789123456789123456
```

In the following example an error message occurs when you configure a password for more than 25 characters when the **service password-encryption** command is enabled.

```
Router(config)# service password-encryption
Router(config)# router bgp 200
Router(config-router)# bgp router-id 2.2.2.2
Router(config-router)# neighbor 209.165.200.225 remote-as 3
Router(config-router)# neighbor 209.165.200.225 password 12345678912345678912345678901
% BGP: Password length must be less than or equal to 25.

Router(config-router)# do show run | i password
service password-encryption
 neighbor 209.165.200.225 password 123456789123456789123456
```

Related Commands

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

neighbor peer-group (assigning members)

To configure a BGP neighbor to be a member of a peer group, use the **neighbor peer-group** command in address family or router configuration mode. To remove the neighbor from the peer group, use the **no** form of this command.

neighbor {*ip-address* | *ipv6-address*} **peer-group** *peer-group-name*

no neighbor {*ip-address* | *ipv6-address*} **peer-group** *peer-group-name*

Syntax Description

ip-address	IP address of the BGP neighbor that belongs to the peer group specified by the *peer-group-name argument*.
ipv6-address	IPv6 address of the BGP neighbor that belongs to the peer group specified by the *peer-group-name argument*.
peer-group-name	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.
12.2(2)T	Support for IPv6 was added.
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.
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.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

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

Note Using the **no** form of the **neighbor peer-group** command removes all of the BGP configuration for that neighbor, not just the peer group association.

Examples

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

```
router bgp 100
 neighbor internal peer-group
 neighbor internal remote-as 100
 neighbor internal update-source loopback 0
 neighbor internal route-map set-med out
 neighbor internal filter-list 1 out
 neighbor internal filter-list 2 in
 neighbor 172.16.232.53 peer-group internal
 neighbor 172.16.232.54 peer-group internal
 neighbor 172.16.232.55 peer-group internal
 neighbor 172.16.232.55 filter-list 3 in
```

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

```
router bgp 100
address-family ipv4 unicast
 neighbor internal peer-group
 neighbor internal remote-as 100
 neighbor internal update-source loopback 0
 neighbor internal route-map set-med out
 neighbor internal filter-list 1 out
 neighbor internal filter-list 2 in
 neighbor 172.16.232.53 peer-group internal
 neighbor 172.16.232.54 peer-group internal
 neighbor 172.16.232.55 peer-group internal
 neighbor 172.16.232.55 filter-list 3 in
```

Related Commands

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

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

Router configuration

Command History

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

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
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
clear ip bgp peer-group	Removes all the members of a BGP peer group.
show ip bgp peer-group	Displays information about BGP peer groups.

neighbor prefix-length-size

To specify the length (in bytes) of the prefix length field of prefixes being advertised to a neighbor, use the **neighbor prefix-length-size** command in L2VPN VPLS address-family configuration mode. To restore the default value, use the **no** form of this command.

neighbor *ip-address* **prefix-length-size {1|2}**

no neighbor *ip-address* **prefix-length-size**

Syntax Description

ip-address	IP address of the neighbor to which the router is advertising prefixes.
1|2	Specifies the length in bytes of the prefix length field (either 1 byte or 2 bytes).

Command Default

1 byte

Command Modes

L2VPN VPLS address-family configuration (config-router-af)

Command History

Release	Modification
12.2(33)SRD	This command was introduced.

Usage Guidelines

You might need to configure this command for interoperability with Juniper's JunOS. If the neighbor is a Juniper JunOS router, change the prefix length size to 2 bytes.

The size of the prefix length field is either 1 or 2 bits or bytes, depending on the address family of the prefix, as follows:

Address Family	Prefix Length Measured In	Prefix Length
All other address families	Bits	1
L2VPN AF (old Cisco)	Bits	1
L2VPN AF (AB76)	Bits (default, no prefix-length-size)	1
L2VPN AF (AB76)	Bytes (with prefix-length-size 2)	2
L2VPN AF (JUNOS)	Bytes	2

Examples

The following example configures the prefix length size to 2 bytes for L2VPN VPLS prefixes advertised to the neighbor at 10.1.1.1.

```
router bgp 1600
 address-family l2vpn vpls
 neighbor 10.1.1.1 prefix-length-size 2
 neighbor 10.1.1.1 activate
 exit-address-family
```

Related Commands

Command	Description
address-family l2vpn vpls	Enters address family configuration mode to configure a routing session using Layer 2 Virtual Private Network (L2VPN) endpoint provisioning address information.
prefix-length-size	Specifies the length (in bytes) of the prefix length field of prefixes being advertised to neighbors.

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

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

Command Default

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

Command Modes

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 *prefix-list-name* argument was amended to specify the name of a CLNS filter expression or a CLNS filter set.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
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.
Cisco IOS XE 2.6	This command was integrated into Cisco IOS XE Release 2.6.

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
address-family ipv4 (BGP)	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.

address-family vpnv4	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.
clear ip prefix-list	Resets the hit count of the prefix list entries.
clns filter-expr	Creates an entry in a CLNS filter expression.
clns filter-set	Creates an entry in a CLNS filter set.
ip as-path access-list	Defines a BGP-related access list.
ip prefix-list	Creates an entry in a prefix list.
ip prefix-list description	Adds a text description of a prefix list.
ip prefix-list sequence-number	Enables the generation of sequence numbers for entries in a prefix list.
neighbor filter-list	Sets up a BGP filter.
show bgp nsap filter-list	Displays information about a filter list or filter list entries.
show ip bgp peer-group	Displays information about BGP peer groups.
show ip prefix-list	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* | *ipv6-address*[**%**] | *peer-group-name*} **remote-as** *autonomous-system-number* [**alternate-as** *autonomous-system-number ...*]

no neighbor {*ip-address* | *ipv6-address*[**%**] | *peer-group-name*} **remote-as** *autonomous-system-number* [**alternate-as** *autonomous-system-number ...*]

Syntax Description

ip-address	IP address of the neighbor.
ipv6-address	IPv6 address of the neighbor.
%	(Optional) IPv6 link-local address identifier. This keyword needs to be added whenever a link-local IPv6 address is used outside the context of its interface.
peer-group-name	Name of a BGP peer group.
autonomous-system-number	Number of an autonomous system to which the neighbor belongs 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. When used with the **alternate-as** keyword, up to five autonomous system numbers may be entered.
alternate-as	(Optional) Specifies an alternate autonomous system in which a potential dynamic neighbor can be identified. Up to five autonomous system numbers may be entered when this keyword is specified.

Command Default

There are no BGP or multiprotocol BGP neighbor peers.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
10.0	This command was introduced.
11.0	The *peer-group-name* argument was added.

Release	Modification
11.1(20)CC	The **nlri unicast**, **nlri multicast**, and **nlri unicast multicast** keywords were added.
12.0(7)T	The **nlri unicast**, **nlri multicast**, and **nlri unicast multicast** keywords were removed.
12.2(4)T	Support for the IPv6 address family was added.
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.
12.2(33)SRB	This command was modified. The **%** keyword was added.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH. The **alternate-as** keyword was added to support BGP dynamic neighbors.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
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.
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 integrated into Cisco IOS Release 15.0(1)S.

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 in the appropriate address family configuration mode.

Use the **alternate-as** keyword introduced in Cisco IOS Release 12.2(33)SXH to specify up to five alternate autonomous systems in which a dynamic BGP neighbor may be identified. BGP dynamic neighbor support allows BGP peering to a group of remote neighbors that are defined by a range of IP addresses. BGP dynamic neighbors are configured using a range of IP addresses and BGP peer groups. After a subnet range is configured and associated with a BGP peer group using the **bgp listen** command and a TCP session is initiated for an IP address in the subnet range, a new BGP neighbor is dynamically created as a member of that group. The new BGP neighbor will inherit any configuration or templates for the group.

The **%** keyword is used whenever link-local IPv6 addresses are used outside the context of their interfaces. This keyword does not need to be used for non-link-local IPv6 addresses.

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 followed by the **clear ip bgp *** command to perform a hard reset of all current BGP sessions.

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.

Note In Cisco IOS releases that include 4-byte ASN support, command accounting and command authorization that include a 4-byte ASN number are sent in the asplain notation irrespective of the format that is used on the command-line interface.

To ensure a smooth transition, we recommend that all BGP speakers within an autonomous system that is identified using a 4-byte autonomous system number, be upgraded to support 4-byte autonomous system numbers.

Examples

The following example specifies that a router at the address 10.108.1.2 is an internal BGP (iBGP) neighbor in autonomous system number 65200:

```
router bgp 65200
 network 10.108.0.0
 neighbor 10.108.1.2 remote-as 65200
```

The following example specifies that a router at the IPv6 address 2001:0DB8:1:1000::72a is an external BGP (eBGP) neighbor in autonomous system number 65001:

```
router bgp 65300
 address-family ipv6 vrf site1
 neighbor 2001:0DB8:1:1000::72a remote-as 65001
```

The following example assigns a BGP router to autonomous system 65400, 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 is a remote router in a different autonomous system from the router on which this configuration is entered (an eBGP neighbor); the second **neighbor remote-as** command shows an internal BGP 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 from the router on which this configuration is entered (also an eBGP neighbor).

```
router bgp 65400
 network 10.108.0.0
 network 192.168.7.0
 neighbor 10.108.200.1 remote-as 65200
 neighbor 10.108.234.2 remote-as 65400
 neighbor 172.29.64.19 remote-as 65300
```

The following example configures neighbor 10.108.1.1 in autonomous system 65001 to exchange only multicast routes:

```
router bgp 65001
 neighbor 10.108.1.1 remote-as 65001
 neighbor 172.31 1.2 remote-as 65001
 neighbor 172.16.2.2 remote-as 65002
 address-family ipv4 multicast
  neighbor 10.108.1.1 activate
  neighbor 172.31 1.2 activate
  neighbor 172.16.2.2 activate
  exit-address-family
```

The following example configures neighbor 10.108.1.1 in autonomous system 65001 to exchange only unicast routes:

```
router bgp 65001
 neighbor 10.108.1.1 remote-as 65001
 neighbor 172.31 1.2 remote-as 65001
 neighbor 172.16.2.2 remote-as 65002
```

The following example, configurable only in Cisco IOS Release 12.2(33)SXH and later releases, configures a subnet range of 192.168.0.0/16 and associates this listen range with a BGP peer group. Note that the listen range peer group that is configured for the BGP dynamic neighbor feature can be activated in the IPv4 address family using the **neighbor activate** command. After the initial configuration on Router 1, when Router 2 starts a BGP router session and adds Router 1 to its BGP neighbor table, a TCP session is initiated, and Router 1 creates a new BGP neighbor dynamically because the IP address of the new neighbor is within the listen range subnet.

Router 1

```
enable
configure terminal
router bgp 45000
 bgp log-neighbor-changes
 neighbor group192 peer-group
 bgp listen range 192.168.0.0/16 peer-group group192
 neighbor group192 remote-as 40000 alternate-as 50000
 address-family ipv4 unicast
 neighbor group192 activate
 end
```

Router 2

```
enable
configure terminal
router bgp 50000
 neighbor 192.168.3.1 remote-as 45000
 exit
```

If the **show ip bgp summary** command is now entered on Router 1, the output shows the dynamically created BGP neighbor, 192.168.3.2.

```
Router1# show ip bgp summary

BGP router identifier 192.168.3.1, local AS number 45000
BGP table version is 1, main routing table version 1

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
*192.168.3.2    4 50000       2       2        0    0    0 00:00:37        0
* Dynamically created based on a listen range command
Dynamically created neighbors: 1/(200 max), Subnet ranges: 1

BGP peergroup group192 listen range group members:
  192.168.0.0/16
```

The following example configures a BGP process for autonomous system 65538 and configures two external BGP neighbors in different autonomous systems using 4-byte autonomous system numbers in asplain format. This example is supported only on 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 later releases.

```
router bgp 65538
 neighbor 192.168.1.2 remote-as 65536
 neighbor 192.168.3.2 remote-as 65550
 neighbor 192.168.3.2 description finance
 !
 address-family ipv4
  neighbor 192.168.1.2 activate
  neighbor 192.168.3.2 activate
  no auto-summary
  no synchronization
  network 172.17.1.0 mask 255.255.255.0
  exit-address-family
```

The following example configures a BGP process for autonomous system 1.2 and configures two external BGP neighbors in different autonomous systems using 4-byte autonomous system numbers in asdot format. 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, Cisco IOS XE Release 2.3, or a later release.

```
router bgp 1.2
 neighbor 192.168.1.2 remote-as 1.0
 neighbor 192.168.3.2 remote-as 1.14
 neighbor 192.168.3.2 description finance
 !
 address-family ipv4
  neighbor 192.168.1.2 activate
  neighbor 192.168.3.2 activate
  no auto-summary
  no synchronization
  network 172.17.1.0 mask 255.255.255.0
  exit-address-family
```

Related Commands

Command	Description
bgp asnotation dot	Changes the default display and the regular expression match format of BGP 4-byte autonomous system numbers from asplain (decimal values) to dot notation.
bgp listen	Associates a subnet range with a BGP peer group and activates the BGP dynamic neighbors feature.

neighbor peer-group	Creates a BGP peer group.
router bgp	Configures the BGP routing process.

neighbor remove-private-as

To remove private autonomous system numbers from tin eBGP outbound routing updates, use the **neighbor remove-private-as** command in router configuration, address family configuration, or peer-group template mode. To disable this function, use the **no** form of this command.

neighbor {*ip-address* | *peer-group-name*} **remove-private-as** [**all** [**replace-as**]]

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

Syntax Description

ip-address	IP address of the BGP-speaking neighbor.
peer-group-name	Name of a BGP peer group.
all	(Optional) Removes all private AS numbers from the AS path in outgoing updates.
replace-as	(Optional) As long as the **all** keyword is specified, the **replace-as** keyword causes all private AS numbers in the AS path to be replaced with the router's local AS number.

Command Default

No private AS numbers are removed from the AS path.

Command Modes

Router configuration
Address family configuration [Release 15.1(2)T and later]
Peer-group template [Release 15.1(2)T and later]

Command History

Release	Modification
10.3	This command was introduced.
11.0	The *peer-group-name* argument 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.
15.1(2)T	This command was modified. The **all** keyword and the **replace-as** keyword were added.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

This command is available for external BGP (eBGP) neighbors only. The private AS values are 64512 to 65535.

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

Behavior Before Release 15.1(2)T

- If the AS path includes both private and public AS numbers, the software considers this to be a configuration error and does not remove the private AS numbers.
- If the AS path contains the AS number of the eBGP neighbor, the private AS numbers are not removed.
- If this command is used with confederation, it will work as long as the private AS numbers follow the confederation portion of the AS path.

Behavior in Release 15.1(2)T and Later

- The **neighbor remove-private-as** command removes private AS numbers from the AS path even if the path contains both public and private ASNs.
- The **neighbor remove-private-as** command removes private AS numbers even if the AS path contains only private AS numbers. There is no likelihood of a 0-length AS path because this command can be applied to eBGP peers only, in which case the AS number of the local router is appended to the AS path.
- The **neighbor remove-private-as** command removes private AS numbers even if the private ASNs appear before the Confederation segments in the AS path.
- Upon removing private AS numbers from the AS path, the path length of prefixes being sent out will decrease. Because the AS path length is a key element of BGP best path selection, it might be necessary to retain the path length. The **replace-as** keyword ensures that the path length is retained by replacing all removed AS numbers with the local router's AS number.
- The feature can be applied to neighbors per address family. Therefore, you can apply the feature to a neighbor in one address family and not in another, affecting update messages on the outbound side for only the address family for which the feature is configured.

Examples

The following example shows a configuration that removes the private AS number from the updates sent to 172.16.2.33. The result is that the AS path for the paths advertised by 10.108.1.1 through AS 100 will contain only "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
```

The following is an example of removing and replacing private ASNs using Cisco IOS Release 15.1(2)T or later. In this example, when Router A sends prefixes to the peer 172.30.0.7, all private ASNs in the AS path are replaced with the router's own ASN, which is 100.

Router A

```
router bgp 100
 bgp log-neighbor-changes
 neighbor 172.16.101.1 remote-as 1001
 neighbor 172.16.101.1 update-source Loopback0
 neighbor 172.30.0.7 remote-as 200
 neighbor 172.30.0.7 remove-private-as all replace-as
 no auto-summary
```

Router A receives 1.1.1.1 from peer 172.16.101.1, which has some private ASNs (65200, 65201, and 65201) in the AS path list, as shown in the following output:

```
RouterA# show ip bgp 1.1.1.1

BGP routing table entry for 1.1.1.1/32, version 2
Paths: (1 available, best #1, table default)
   Advertised to update-groups:
      1          2
   1001 65200 65201 65201 1002 1003 1003
     172.16.101.1 from 172.16.101.1 (172.16.101.1)
       Origin IGP, localpref 100, valid, external, best RouterA#
```

Because Router A is configured with **neighbor 172.30.0.7 remove-private-as all replace-as**, Router A sends prefix 1.1.1.1 with all private ASNs replaced with 100:

Router B

```
RouterB# show ip bgp 1.1.1.1

BGP routing table entry for 1.1.1.1/32, version 3
Paths: (1 available, best #1, table default)
   Not advertised to any peer
   100 1001 100 100 100 1002 1003 1003
     172.30.0.6 from 172.30.0.6 (192.168.1.2)
       Origin IGP, localpref 100, valid, external, best RouterB#
```

Router B

```
router bgp 200
 bgp log-neighbor-changes
 neighbor 172.30.0.6 remote-as 100
 no auto-summary
```

Related Commands

Command	Description
neighbor remote-as	Allows entries to the BGP neighbor table.
show ip bgp neighbor	Displays entries in the BGP routing table.
show ip bgp update-group	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* | *ipv6-address* [**%**]} **route-map** *map-name* {**in** | **out**}

no neighbor {*ip-address* | *peer-group-name* | *ipv6-address* [**%**]} **route-map** *map-name* {**in** | **out**}

Syntax Description

ip-address	IP address of the neighbor.
peer-group-name	Name of a BGP or multiprotocol BGP peer group.
ipv6-address	IPv6 address of the neighbor.
%	(Optional) IPv6 link-local address identifier. This keyword needs to be added whenever a link-local IPv6 address is used outside the context of its interface.
map-name	Name of a route map.
in	Applies route map to incoming routes.
out	Applies route map to outgoing routes.

Command Default

No route maps are applied to a peer.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
10.0	This command was introduced.
12.0(7)T	Address family configuration mode was added.
12.2(4)T	Support for IPv6 was added.
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.
12.2(33)SRB	The **%** keyword was added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
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.

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 IPv4 or IPv6 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.

The **%** keyword is used whenever link-local IPv6 addresses are used outside the context of their interfaces. This keyword does not need to be used for non-link-local IPv6 addresses.

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 5
 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 5
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
address-family ipv4 (BGP)	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.
address-family ipv6	Enters address family configuration mode for configuring routing sessions such as BGP that use standard IPv6 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPN Version 4 address prefixes.
address-family vpnv6	Places the router in address family configuration mode for configuring routing sessions that use standard VPNv6 address prefixes.
neighbor remote-as	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* | *ipv6-address* | *peer-group-name*} **route-reflector-client**

no neighbor {*ip-address* | *ipv6-address* | *peer-group-name*} **route-reflector-client**

Syntax Description

ip-address	IP address of the BGP neighbor being identified as a client.
ipv6-address	IPv6 address of the BGP neighbor being identified as a client.
peer-group-name	Name of a BGP peer group.

Command Default

There is no route reflector in the autonomous system.

Command Modes

Address family configuration (config-router-af)
Router configuration (config-router)

Command History

Release	Modification
11.1	This command was introduced.
12.0(7)T	Address family configuration mode was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	The *ipv6-address* and *peer-group-name* arguments were added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 3.1S	This command was updated. It was integrated into Cisco IOS XE Release 3.1S.

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 5
 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 5
address-family ipv4 unicast
 neighbor 172.16.70.24 route-reflector-client
```

Related Commands

Command	Description
address-family ipv4 (BGP)	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.
address-family ipv6	Enters address family configuration mode for configuring routing sessions such as BGP that use standard IPv6 address prefixes.
address-family vpnv6	Places the router in address family configuration mode for configuring routing sessions such as BGP that use standard VPNv6 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPN Version 4 address prefixes.
address-family vpnv6	Places the router in address family configuration mode for configuring routing sessions such as BGP that use standard VPNv6 address prefixes.
bgp client-to-client reflection	Restores route reflection from a BGP route reflector to clients.
bgp cluster-id	Configures the cluster ID if the BGP cluster has more than one route reflector.
neighbor route-reflector-client	Configures the router as a BGP route reflector and configures the specified neighbor as its client.
show bgp ipv6	Displays entries in the IPv6 BGP routing table.
show ip bgp	Displays entries in the BGP routing table.

neighbor route-server-client

To specify on a BGP route server that a neighbor is a route server client, use the **neighbor route-server-client** command in IPv4 or IPv6 address family configuration mode. To remove that neighbor as a route server client, use the **no** form of this command.

neighbor {*ipv4-address* | *ipv6-address*} **route-server-client** [**context** *context-name*]

no neighbor {*ipv4-address* | *ipv6-address*} **route-server-client** [**context** *context-name*]

Syntax Description

ipv4-address	IPv4 address of a BGP neighbor.
ipv6-address	IPv6 address of a BGP neighbor.
context *context-name*	(Optional) Assigns a route server context to the specified neighbor. Specify the name of a route server context, which you configure in the **route-server-context** command, when you want flexible policy handling.

Command Default

There are no BGP route servers or BGP route server clients.

Command Modes

IPv4 or IPv6 address family configuration (config-router-af)

Command History

Release	Modification
Cisco IOS XE 3.3S	This command was introduced.

Usage Guidelines

Use this command on a BGP route server to specify the neighbors that are route server clients.

If you want to configure flexible policy handling, you must create a route server context, which includes an import map. The import map points to a route map. The route map points to one or more **match** commands. The **match** command in the example below matches on autonomous system numbers by pointing to an access list. The access list is configured with at least one **permit** statement. The access list that is based on autonomous system numbers is configured by the **ip as-path access-list** command.

Examples

In the following example, the local router is a BGP route server. Its neighbors at 10.0.0.1 and 10.0.0.5 are its route server clients. This example enables basic route server functionality (nexthop, AS-path, and MED transparency).

```
router bgp 900
 neighbor 10.0.0.1 remote-as 100
 neighbor 10.0.0.5 remote-as 500
 address-family ipv4 unicast
 neighbor 10.0.0.1 route-server-client
 neighbor 10.0.0.5 route-server-client
 neighbor 10.0.0.1 activate
 neighbor 10.0.0.5 activate
```

In the following example, the local router is a BGP route server. Its neighbors at 10.10.10.12 and 10.10.10.13 are its route server clients. A route server context named ONLY_AS27_CONTEXT is created and applied to the neighbor at 10.10.10.13. The context uses an import map that references a route map named only_AS27_routemap. The route map matches routes permitted by access list 27. Access list 27 permits routes that have 27 in the autonomous system path.

```
router bgp 65000
   route-server-context ONLY_AS27_CONTEXT
      address-family ipv4 unicast
         import-map only_AS27_routemap
      exit-address-family
   exit-route-server-context
   !
   neighbor 10.10.10.12 remote-as 12
   neighbor 10.10.10.12 description Peer12
   neighbor 10.10.10.13 remote-as 13
   neighbor 10.10.10.13 description Peer13
   neighbor 10.10.10.21 remote-as 21
   neighbor 10.10.10.27 remote-as 27
   !
   address-family ipv4
      neighbor 10.10.10.12 activate
      neighbor 10.10.10.12 route-server-client
      neighbor 10.10.10.13 activate
      neighbor 10.10.10.13 route-server-client context ONLY_AS27_CONTEXT
      neighbor 10.10.10.21 activate
      neighbor 10.10.10.27 activate
   exit-address-family
!
ip as-path access-list 27 permit 27
!
route-map only_AS27_routemap permit 10
   match as-path 27
!
```

Related Commands

Command	Description
route-server-context	Creates a route-server context in order to provide flexible policy handling for a BGP route server

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* | *ipv6-address* | *peer-group-name*} **send-community** [**both** | **standard** | **extended**]

no neighbor {*ip-address* | *ipv6-address* | *peer-group-name*} **send-community**

Syntax Description

ip-address	IP address of the neighbor.
ipv6-address	IPv6 address of the neighbor.
peer-group-name	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.

Command Default

No communities attribute is sent to any neighbor.

Command Modes

Address family configuration
Router configuration

Command History

Release	Modification
10.3	This command was introduced.
11.0	The *peer-group-name* argument was added.
12.0(7)T	Address family configuration mode was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	The *ipv6-address* argument was added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

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 109 and is configured to send the communities attribute to its neighbor at IP address 172.16.70.23:

```
router bgp 109
 neighbor 172.16.70.23 send-community
```

In the following address family configuration mode example, the router belongs to autonomous system 109 and is configured to send the communities attribute to its neighbor at IP address 172.16.70.23:

```
router bgp 109
address-family ipv4 multicast
 neighbor 172.16.70.23 send-community
```

Related Commands

Command	Description
address-family ipv4 (BGP)	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.
address-family ipv6	Places the router in address family configuration mode for configuring routing sessions such as BGP that use standard IPv6 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPN Version 4 address prefixes.
address-family vpnv6	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard VPNv6 address prefixes.
match community	Matches a BGP community.
neighbor remote-as	Creates a BGP peer group.
set community	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

ip-address	IP address of the neighbor.
peer-group-name	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.
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 **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

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

neighbor slow-peer detection

To specify a threshold time that dynamically determines a slow peer, use the **neighbor slow-peer detection** command in address-family configuration mode. To remove dynamic slow peer detection for a neighbor, use the **no** form of this command.

neighbor {*neighbor-address* | *peer-group-name*} **slow-peer detection** [**disable** | **threshold** *seconds*]

no neighbor {*neighbor-address* | *peer-group-name*} **slow-peer detection**

Syntax Description

neighbor-address	IP address of a BGP neighbor whose update messages are being compared to the current time to determine slowness.
peer-group-name	Peer group name of the bgp neighbors whose update messages are being compared to the current time to determine slowness.
disable	(Optional) Disables slow peer detection for the specified neighbor even if slow peer detection is enabled at the global, address-family level.
threshold *seconds*	(Optional) Threshold time in seconds that the timestamp of the oldest message in a peers queue can be lagging behind the current time before the peer is determined to be a slow peer. The range is from 120 to 3600; the default is 300.

Command Default

No neighbor is configured as a dynamic slow peer.

Command Modes

Address-family configuration (config-router-af)

Command History

Release	Modification
15.0(1)S	This command was introduced.
Cisco IOS XE 3.1S	This command was introduced.

Usage Guidelines

Update messages are timestamped when they are formatted. The timestamp of the oldest message in a peers queue is compared to the current time to determine if the peer is lagging more than the configured number of seconds. When a peer is dynamically detected to be a slow peer, the system will send a syslog message. The peer will be marked as recovered and another syslog message will be generated only after the peer's update group converges.

You can use this command alone just to detect a slow peer, or you can use this command with the **neighbor slow-peer split-update-group dynamic** command to move the peer to a slow update group.

Note The **neighbor slow-peer detection** command performs the same function as the **bgp slow-peer detection** command (at the address-family level). The **neighbor slow-peer detection** command overrides the global, address-family level command. If the **neighbor slow-peer detection** command is unconfigured or if **no neighbor slow-peer detection** is configured, the system will inherit the global, address-family level configuration.

Note The **slow-peer detection** command performs the same function through a peer policy template.

Examples

The following example sets a threshold of 400 seconds for the BGP peer at 10.4.4.4. Once the current time is more than 400 seconds later than the timestamp on the oldest message in that peers queue, the peer is determined to be a slow peer.

```
Router(config-router)# address-family ipv4
Router(config-router-af)# neighbor 10.4.4.4 slow-peer detection threshold 400
Router(config-router-af)# neighbor 10.4.4.4 slow-peer split-update-group dynamic
```

In the following example, both neighbors 4.4.4.4 and 6.6.6.6 have slow peer detection enabled for them due to the global command **bgp slow-peer detection**:

```
Router(config)# router bgp 100
Router(config-router)# bgp log-neighbor-changes
Router(config-router)# neighbor 4.4.4.4 remote-as 100
Router(config-router)# neighbor 6.6.6.6 remote-as 100
Router(config-router)# address-family ipv4
Router(config-router-af)# bgp slow-peer detection
Router(config-router-af)# neighbor 4.4.4.4 activate
Router(config-router-af)# neighbor 6.6.6.6 activate
Router(config-router-af)# no auto-summary
Router(config-router-af)# exit-address-family
Router(config-router)#
```

To disable slow peer detection for a particular peer, use the **disable** keyword. The following example disables slow peer detection for the neighbor 4.4.4.4:

```
Router(config)# router bgp 100
Router(config-router)# bgp log-neighbor-changes
Router(config-router)# neighbor 4.4.4.4 remote-as 100
Router(config-router)# neighbor 6.6.6.6 remote-as 100
Router(config-router)# address-family ipv4
Router(config-router-af)# bgp slow-peer detection
Router(config-router-af)# neighbor 4.4.4.4 activate
Router(config-router-af)# neighbor 4.4.4.4 slow-peer detection disable
Router(config-router-af)# neighbor 6.6.6.6 activate
Router(config-router-af)# no auto-summary
Router(config-router-af)# exit-address-family
Router(config-router)#
```

Related Commands

Command	Description
bgp slow-peer detection	Specifies a threshold time that dynamically determines a slow peer at the global, address family level.
clear ip bgp slow	Moves dynamically configured slow peers back to their original update groups.
neighbor slow-peer split-update-group dynamic	Moves a dynamically detected slow peer to a slow update group.

neighbor slow-peer split-update-group dynamic

To move a dynamically detected slow peer to a slow update group, use the **neighbor slow-peer split-update-group dynamic** command in address-family configuration mode. To cancel this method of moving dynamically detected slow peers to a slow update group, use the **no** form of this command.

neighbor {*neighbor-address* | *peer-group-name*} **slow-peer split-update-group dynamic** [**permanent** | **disable**]

no neighbor {*neighbor-address* | *peer-group-name*} **slow-peer split-update-group dynamic**

Syntax Description

neighbor-address	IP address of a BGP neighbor peer that is moved to the slow peer group if dynamically determined to be slow.
peer-group-name	Peer group name of the BGP neighbor peers that are moved to the slow peer group if dynamically determined to be slow.
permanent	(Optional) Specifies that after the slow peer becomes a regular peer (converges), it is not moved back to its original update group automatically. The network administrator can use one of the **clear** commands to move the peer to its original update group.
disable	(Optional) Disables slow peer protection for the specified neighbor even if slow peer protection is enabled at the global, address-family level.

Command Default

No dynamically detected slow peer is moved to a slow peer update group.

Command Modes

Address-family configuration (config-router-af)

Command History

Release	Modification
15.0(1)S	This command was introduced.
Cisco IOS XE 3.1S	This command was introduced.

Usage Guidelines

When a peer is dynamically detected to be a slow peer, the slow peer is moved to a slow update group. If a *static* slow peer update group exists, the dynamic slow peer is moved to the static slow peer update group; otherwise, a new slow peer updated group is created and the peer is moved to that group.

- If the **permanent** keyword is not configured, the slow peer will be moved back to its regular original update group after it becomes a regular peer (converges).
- If the **permanent** keyword is configured, the peer is not automatically moved to its original update group. You can use one of the **clear** commands to move the peer back to its original update group.

If no slow peer detection is configured, the detection will be done at the default threshold of 300 seconds.

The **neighbor slow-peer-split-update-group dynamic** command will override the global configuration. However, if the **no neighbor slow-peer-split-update-group dynamic** command is configured, then the peers will inherit the global address family configuration specified by the **bgp slow-peer detection** command.

Examples

In the following example, the timestamp of the oldest message in a peers queue is compared to the current time to determine if the peer is lagging more than 360 seconds. If it is, the neighbor who sent the message is determined to be a slow peer, and is put in the slow peer update group. Because the **permanent** keyword is not configured, the slow peer will be moved back to its regular original update group after it becomes a regular peer (converges).

```
Router(config-router)# address-family ipv4
Router(config-router-af)# neighbor 10.4.4.4 slow-peer detection threshold 360
Router(config-router-af)# neighbor 10.4.4.4 slow-peer split-update-group dynamic
```

In the following example, both neighbors 4.4.4.4 and 6.6.6.6 have slow peer protection enabled for them due to the global command **bgp slow-peer split-update-group dynamic**:

```
Router(config)# router bgp 100
Router(config-router)# bgp log-neighbor-changes
Router(config-router)# neighbor 4.4.4.4 remote-as 100
Router(config-router)# neighbor 6.6.6.6 remote-as 100
Router(config-router)# address-family ipv4
Router(config-router-af)# bgp slow-peer split-update-group dynamic
Router(config-router-af)# neighbor 4.4.4.4 activate
Router(config-router-af)# neighbor 6.6.6.6 activate
Router(config-router-af)# no auto-summary
Router(config-router-af)# exit-address-family
Router(config-router)#
```

To disable slow peer protection for a particular peer, use the **disable** keyword. The following example disables slow peer protection for the neighbor 4.4.4.4:

```
Router(config)# router bgp 100
Router(config-router)# bgp log-neighbor-changes
Router(config-router)# neighbor 4.4.4.4 remote-as 100
Router(config-router)# neighbor 6.6.6.6 remote-as 100
Router(config-router)# address-family ipv4
Router(config-router-af)# bgp slow-peer detection
Router(config-router-af)# neighbor 4.4.4.4 activate
Router(config-router-af)# neighbor 4.4.4.4 slow-peer split-update-group dynamic disable
Router(config-router-af)# neighbor 6.6.6.6 activate
Router(config-router-af)# no auto-summary
Router(config-router-af)# exit-address-family
Router(config-router)#
```

Related Commands

Command	Description
clear ip bgp slow	Moves dynamically configured slow peers back to their original update groups.
neighbor slow-peer detection	Specifies a threshold time that dynamically determines a slow peer in neighbor address family configuration mode.

neighbor slow-peer split-update-group static

To mark a BGP neighbor as a slow peer and move it to a slow update group, use the **neighbor slow-peer split-update-group static** command in address-family configuration mode. To unmark the slow peer and return it to its original update group, use the **no** form of this command.

neighbor {*neighbor-address* | *peer-group-name*} **slow-peer split-update-group static**

no neighbor {*neighbor-address* | *peer-group-name*} **slow-peer split-update-group static**

Syntax Description

neighbor-address	IP address of a BGP neighbor peer that is marked as slow and moved to a slow peer group.
peer-group-name	Peer group name of the BGP neighbor peers that are marked as slow and moved to a slow peer group.

Command Default

No peer is statically marked as slow and moved to a slow peer update group, unless through a peer policy template or configured at neighbor or peer group.

Command Modes

Address-family configuration (config-router-af)

Command History

Release	Modification
15.0(1)S	This command was introduced.
Cisco IOS XE 3.1S	This command was introduced.

Usage Guidelines

Configure a static slow peer when the peer is known to be slow (perhaps due to a slow link or low processing power).

The **slow-peer split-update-group static** command performs the same function through a peer policy template.

Examples

In the following example, the neighbor with the specified IP address is marked as a slow peer and is moved to a slow update group.

```
Router(config-router)# address-family ipv4
Router(config-router-af)# neighbor 172.20.2.2 slow-peer split-update-group static
```

Related Commands

Command	Description
slow-peer split-update-group static	Marks a BGP neighbor as a static slow peer and moves it to a slow update group.

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

ip-address	IP address of the BGP-speaking neighbor.
peer-group-name	Name of a BGP peer group.
inbound	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.
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

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
clear ip bgp	Resets a BGP connection using BGP soft reconfiguration.
neighbor remote-as	Creates a BGP peer group.
show ip bgp neighbors	Display information about the TCP and BGP connections to neighbors.

neighbor soo

To set the site-of-origin (SoO) value for a Border Gateway Protocol (BGP) neighbor or peer group, use the **neighbor soo** command in address family IPv4 VRF configuration mode. To remove the SoO value for a BGP neighbor or peer group, use the **no** form of this command.

neighbor {*ip-address* | *peer-group-name*} **soo** *extended-community-value*

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

Syntax Description

ip-address	IP address of a neighboring router.
peer-group-name	Name of a BGP peer group.
extended-community-value	Specifies the VPN extended community value. The value takes one of the following formats: • A 16-bit autonomous system number, a colon, and a 32-bit number, for example: 45000:3 • A 32-bit IP address, a colon, and a 16-bit number, for example: 192.168.10.2:51 In Cisco IOS Release 12.4(24)T, 4-byte autonomous system numbers are supported in the range from 1.0 to 65535.65535 in asdot notation only. In 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. For more details about autonomous system number formats, see the **router bgp** command.

Command Default

No SoO value is set for a BGP neighbor or peer group.

Command Modes

Address family IPv4 VRF configuration (config-router-af)

Command History

Release	Modification
12.4(11)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
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 2.4	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
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.

Usage Guidelines

Use this command to set the SoO value for a BGP neighbor. The SoO value is set under address family IPv4 VRF configuration mode either directly for a neighbor or for a BGP peer group.

The SoO extended community is a BGP extended community attribute that is used to identify routes that have originated from a site so that the readvertisement of that prefix back to the source site can be prevented. The SoO extended community uniquely identifies the site from which a router has learned a route. BGP can use the SoO value associated with a route to prevent routing loops.

In releases prior to Cisco IOS Release 12.4(11)T, 12.2(33)SRB, and 12.2(33)SB, the SoO extended community attribute is configured using an inbound route map that sets the SoO value during the update process. The introduction of the **neighbor soo** and **soo** commands simplifies the SoO value configuration.

Note A BGP neighbor or peer policy template-based SoO configuration takes precedence over an SoO value configured in an inbound route map.

In Cisco IOS Release 12.4(24)T, 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.

In 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 followed by the **clear ip bgp *** command to perform a hard reset of all current BGP sessions.

Examples

The following example shows how to configure an SoO value for a BGP neighbor. Under address family IPv4 VRF, a neighbor is identified and an SoO value is configured for the neighbor.

```
router bgp 45000
 address-family ipv4 vrf VRF_SOO
  neighbor 192.168.1.2 remote-as 40000
  neighbor 192.168.1.2 activate
  neighbor 192.168.1.2 soo 45000:40
  end
```

The following example shows how to configure an SoO value for a BGP peer group. Under address family IPv4 VRF, a BGP peer group is configured, an SoO value is configured for the peer group, a neighbor is identified, and the neighbor is configured as a member of the peer group.

```
router bgp 45000
 address-family ipv4 vrf VRF_SOO
  neighbor SOO_GROUP peer-group
  neighbor SOO_GROUP soo 45000:65
  neighbor 192.168.1.2 remote-as 40000
```

```
  neighbor 192.168.1.2 activate
  neighbor 192.168.1.2 peer-group SOO_GROUP
  end
```

The following example shows how to configure an SoO value for a BGP neighbor using 4-byte autonomous system numbers. Under address family IPv4 VRF, a neighbor is identified and an SoO value of 1.2:1 is configured for the neighbor. This example requires Cisco IOS Release 12.4(24)T, Cisco IOS XE Release 2.4, or a later release.

```
router bgp 1.2
 address-family ipv4 vrf site1
  neighbor 192.168.1.2 remote-as 1.14
  neighbor 192.168.1.2 activate
  neighbor 192.168.1.2 soo 1.2:1
  end
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Enters address family configuration mode to configure a routing session using standard IP Version 4 address prefixes.
router bgp	Configures the BGP routing process.
soo	Sets the SoO value for a BGP peer policy template.