clear bgp nsap

To clear and then reset Connectionless Network Service (CLNS) network service access point (NSAP) Border Gateway Protocol (BGP) sessions, use the **clear bgp nsap** command in privileged EXEC mode.

clear bgp nsap {***** | *as-number* | *ip-address*} [**soft**] [**in** | **out**]

Syntax Description

*****	Clears and then resets all current BGP sessions.
as-number	Clears and then resets BGP sessions for BGP neighbors within the specified autonomous system.
ip-address	Clears the TCP connection to the specified BGP neighbor and removes all routes learned from the connection from the BGP table. The TCP connections are then reset.
soft	(Optional) Soft reset. Allows routing tables to be reconfigured and activated without clearing the BGP session.
in | **out**	(Optional) Triggers inbound or outbound soft reconfiguration. If the **in** or **out** option is not specified, both inbound and outbound soft reset are triggered.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

The **clear bgp nsap** command is similar to the **clear ip bgp** command, except that it is NSAP address family-specific.

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

Use the ***** keyword to reset all neighbor sessions. The software will clear and then reset the neighbor connections. Use this form of the command in the following situations:

- BGP timer specification change
- BGP administrative distance changes

Use the **soft out** keywords to clear and reset only the outbound neighbor connections. Inbound neighbor sessions will not be reset. Use this form of the command in the following situations:

- Additions or changes are made to the BGP-related access lists
- BGP-related weights change
- BGP-related distribution lists change
- BGP-related route maps change

Use the **in** keyword to clear only the inbound neighbor connections. Outbound neighbor sessions will not be reset. Use this form of the command in the following situations:

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

Examples

In the following example, the inbound session with the neighbor 172.20.16.6 is cleared without the outbound session being reset:

```
Router# clear bgp nsap 172.20.16.6 in
```

In the following example, a soft clear is applied to outbound sessions with the neighbors in autonomous system 65000 without the inbound session being reset:

```
Router# clear bgp nsap 65000 soft out
```

Related Commands

Command	Description
show bgp nsap	Displays entries in the BGP routing table for the NSAP address family.

clear bgp nsap dampening

To clear Border Gateway Protocol (BGP) route dampening information for the network service access point (NSAP) address family and unsuppress the suppressed routes, use the **clear bgp nsap dampening** command in privileged EXEC mode.

clear bgp nsap dampening [*nsap-prefix*]

Syntax Description

nsap-prefix	(Optional) NSAP prefix about which to clear dampening information. This argument can be up to 20 octets long.

Command Default

When the *nsap-prefix* argument is not specified, the **clear bgp nsap dampening** command clears route dampening information for the entire BGP routing table for the NSAP address family.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

The **clear bgp nsap dampening** command is similar to the **clear ip bgp dampening** command, except that it is specific to the NSAP address family.

Examples

In the following example, route dampening information is cleared for the route to NSAP prefix 49.6001 and locally suppressed routes are unsuppressed:

```
Router# clear bgp nsap dampening 49.6001
```

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes various BGP route dampening factors.
show bgp nsap dampened-paths	Displays BGP dampened routes for the NSAP address family.

clear bgp nsap external

To clear all external BGP (eBGP) peers for the network service access point (NSAP) address family, use the **clear bgp nsap external** command in privileged EXEC mode.

clear bgp nsap external [**soft**] [**in** | **out**]

Syntax Description

soft	(Optional) Soft reset. Does not reset the session.
in | **out**	(Optional) Triggers inbound or outbound soft reconfiguration. If the **in** or **out** option is not specified, both inbound and outbound soft reset are triggered.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

The **clear bgp nsap external** command is similar to the **clear ip bgp external** command, except that it is specific to the NSAP address family.

Examples

In the following example, the inbound sessions with external BGP peers are cleared without the outbound sessions being reset:

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

Related Commands

Command	Description
clear bgp nsap	Resets an NSAP BGP connection by dropping all neighbor sessions.

clear bgp nsap flap-statistics

To clear Border Gateway Protocol (BGP) flap statistics for the network service access point (NSAP) address family, use the **clear bgp nsap flap-statistics** command in privileged EXEC mode.

clear bgp nsap flap-statistics [*nsap-prefix*] [**regexp** *regexp* | **filter-list** *access-list-number*]

Syntax Description

nsap-prefix	(Optional) NSAP prefix about which to clear dampening information. This argument can be up to 20 octets long.
regexp *regexp*	(Optional) Clears flap statistics for all the paths that match the regular expression.
filter-list *access-list-number*	(Optional) Clears flap statistics for all the paths that pass the access list. The acceptable access list number range is from 1 to 199.

Command Default

No statistics are cleared.

If no arguments or keywords are specified, the software clears flap statistics for all routes.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

The **clear bgp nsap flap-statistics** command is similar to the **clear ip bgp flap-statistics** command, except that it is specific to the NSAP address family.

The flap statistics for a route are also cleared when an NSAP BGP peer is reset. Although the reset withdraws the route, no penalty is applied in this instance even though route flap dampening is enabled.

Examples

In the following example, all of the flap statistics for paths that pass access list 3 are cleared:

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

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes various BGP route dampening factors.
show bgp nsap flap-statistics	Displays BGP flap statistics for the NSAP address family.

clear bgp nsap peer-group

To clear the Border Gateway Protocol (BGP) TCP connections to all members of a BGP peer group for the network service access point (NSAP) address family, use the **clear bgp nsap peer-group** command in privileged EXEC mode.

clear bgp nsap peer-group *peer-group-name*

Syntax Description

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

Command Default

No BGP TCP connections are cleared.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

The **clear bgp nsap peer-group** command is similar to the **clear ip bgp peer-group** command, except that it is specific to the NSAP address family.

Examples

In the following example, the BGP TCP connections are cleared for all members of the NSAP BGP peer group named internal:

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

Related Commands

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

clear ip bgp

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

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

Syntax Description

*****	Specifies that all current BGP sessions will be reset.
all	(Optional) Specifies the reset of all address family sessions.
autonomous-system-number	Number of the autonomous system in which all BGP peer sessions will be reset. Number in the range from 1 to 65535. • In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, 4-byte autonomous system numbers are supported in the range from 65536 to 4294967295 in asplain notation and in the range from 1.0 to 65535.65535 in asdot notation. • In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, 4-byte autonomous system numbers are supported in the range from 1.0 to 65535.65535 in asdot notation only. For more details about autonomous system number formats, see the **router bgp** command.
neighbor-address	Specifies that only the identified BGP neighbor will be reset. The value for this argument can be an IPv4 or IPv6 address.
peer-group *group-name*	Specifies that only the identified BGP peer group will be reset.
in	(Optional) Initiates inbound reconfiguration. If neither the **in** nor **out** keywords are specified, both inbound and outbound sessions are reset.
prefix-filter	(Optional) Clears the existing outbound route filter (ORF) prefix list to trigger a new route refresh or soft reconfiguration, which updates the ORF prefix list.
out	(Optional) Initiates inbound or outbound reconfiguration. If neither the **in** nor **out** keywords are specified, both inbound and outbound sessions are reset.
slow	(Optional) Clears slow-peer status forcefully and moves it to original update group.
soft	(Optional) Initiates a soft reset. Does not tear down the session.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.0(2)S	This command was integrated into Cisco IOS Release 12.0(2)S, and dynamic inbound soft reset capability was added.

Release	Modification
12.0(7)T	The dynamic inbound soft reset capability was integrated into Cisco IOS Release 12.0(7)T.
12.0(22)S	The **vpnv4** and **ipv4** keywords were added.
12.0(29)S	The **mdt** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX.
12.0(32)S12	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(24)T	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.3	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SXI1	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
12.2(33)SRE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
15.0(1)S	This command was modified. The **slow** keyword was added.
Cisco IOS XE 3.1S	This command was modified. The **slow** keyword was added.

Usage Guidelines

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

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

Generating Updates from Stored Information

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

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

Use this command whenever any of the following changes occur:

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

Dynamic Inbound Soft Reset

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

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

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

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

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

Examples

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

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

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

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

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

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

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

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

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

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

Related Commands

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

clear ip bgp dampening

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

Syntax Without Address Family Syntax

clear ip bgp [**vrf** *vrf-name*] **dampening** [*network-address*] [*ipv4-mask*]

Syntax With Address Family Syntax

clear ip bgp [**ipv4** {**multicast** | **unicast**}] **dampening** [*network-address*] [*ipv4-mask*]

clear ip bgp [**vrf** *vrf-name*] [**vpnv4 unicast**] **dampening** [**rd** *route-distinguisher*] [*network-address*] [*ipv4-mask*]

Syntax Description

vrf	(Optional) Specifies an instance of a routing table.
vrf-name	(Optional) Name of the Virtual Private Network (VPN) routing and forwarding (VRF) table to use for storing data.
network-address	(Optional) IPv4 address of the network or neighbor to clear dampening information. If no address family keyword is specified when entering the *neighbor-address* argument, you will be prompted for an IPv4 address.
ipv4-mask	(Optional) IPv4 network mask.
ipv4	(Optional) Specifies the reset of IPv4 address family sessions.
multicast	(Optional) Specifies multicast address family sessions.
unicast	(Optional) Specifies unicast address family sessions.
vpn4	(Optional) Specifies the reset of Virtual Private Network Version 4 (VPNv4) address family sessions.
rd *route-distinguisher*	(Optional) Specifies the VPN route distinguisher.

Command Modes

Privileged EXEC (#)

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.
15.1(2)T	This command was modified. The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

The **clear ip bgp dampening** is used to clear stored route dampening information. If no keywords or arguments are entered, route dampening information for the entire routing table is cleared.

Examples

The following example clears route dampening information for VPNv4 address family prefixes from network 192.168.10.0/24 and unsuppress suppressed routes.

```
Router# clear ip bgp vpnv4 unicast dampening 192.168.10.0 255.255.255.0
```

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or configures BGP route dampening parameters.
clear ip bgp flap-statistics	Resets BGP route dampening flap-statistics.
set dampening	Sets set BGP route dampening parameters in a route map.
show ip bgp dampened-paths	Displays BGP dampened routes.

clear ip bgp external

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

Syntax Without Address Family Syntax

clear ip bgp external [**in** [**prefix-filter**]] [**out**] [**soft** [**in** [**prefix-filter**] | **out**]]

Syntax With Address Family Syntax

clear ip bgp external [**all** | **ipv4** {**multicast** | **mdt** | **unicast**} | **ipv6** {**multicast** | **unicast**} | **vpnv4 unicast** | **vpnv6 unicast**] [**in** [**prefix-filter**]] [**out**] [**soft** [**in** [**prefix-filter**] | **out**]]

Syntax Description

in	(Optional) Initiates inbound reconfiguration. If neither the **in** nor **out** keywords are specified, both inbound and outbound sessions are reset.
prefix-filter	(Optional) Clears the existing outbound route filter (ORF) prefix list to trigger a new route refresh or soft reconfiguration, which updates the ORF prefix list.
out	(Optional) Initiates inbound or outbound reconfiguration. If neither the **in** nor **out** keywords are specified, both inbound and outbound sessions are reset.
soft	(Optional) Initiates a soft reset. Does not tear down the session.
all	(Optional) Specifies the reset of eBGP peering sessions for all address families.
ipv4	(Optional) Specifies the reset of eBGP peering sessions for IPv4 address family sessions.
multicast	(Optional) Specifies multicast address family sessions.
mdt	(Optional) Specifies multicast distribution tree (MDT) address family sessions.
unicast	(Optional) Specifies unicast address family sessions.
ipv6	(Optional) Specifies the reset of eBGP peering sessions for IPv6 address family sessions.
vpnv4	(Optional) Specifies the reset of eBGP peering sessions for Virtual Private Network Version 4 (VPNv4) address family sessions.
vpnv6	(Optional) Specifies the reset of eBGP peering sessions for Virtual Private Network Version 6 (VPNv6) address family sessions.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(2)S	This command was introduced.
12.0(22)S	The **vpnv4** and **ipv4** keywords were added.
12.0(29)S	The **mdt** keyword was added.

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

Generating Updates from Stored Information

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

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

Use this command whenever any of the following changes occur:

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

Dynamic Inbound Soft Reset

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

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

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

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

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

Examples

In the following example, a soft reconfiguration is configured for all inbound eBGP peering sessions:

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

In the following example, all outbound address family IPv4 multicast eBGP peering sessions are cleared:

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

Related Commands

Command	Description
clear ip bgp	Resets BGP connections using hard or soft reconfiguration.
neighbor soft-reconfiguration	Configures the Cisco IOS software to start storing updates.
show ip bgp neighbors	Displays information about BGP and TCP connections to neighbors.

clear ip bgp flap-statistics

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

Syntax Without Address Family Syntax

clear ip bgp [**vrf** *vrf-name*] **flap-statistics** [*neighbor-address* [*ipv4-mask*] | **regexp** *regexp* | **filter-list** *extcom-number*]

Syntax With Address Family Syntax

clear ip bgp [*neighbor-address*] [**vrf** *vrf-name*] [**all** | **ipv4** {**multicast** | **mdt** | **unicast**} | **ipv6** {**multicast** | **unicast**} | **vpnv4 unicast** | **vpnv6 unicast**] **flap-statistics**

Syntax Description

neighbor-address	(Optional) Clears flap statistics for the specified IP address. If this argument is placed before **flap-statistics keyword**, the router clears flap statistics for all paths from the specified neighbor or network. The value for this argument can be an IPv4 or IPv6 address.
vrf	(Optional) Specifies an instance of a routing table.
vrf-name	(Optional) Name of the Virtual Private Network (VPN) routing and forwarding (VRF) table to use for storing data.
ipv4-mask	(Optional) IPv4 network mask.
regexp	(Optional) Clears flap statistics for all the paths that match the regular expression.
regexp	(Optional) Regular expression.
filter-list	(Optional) Clears flap statistics for all the paths that pass the access list. The access list is specified using an extended community list number.
extcom-number	(Optional) Extended community list number.
all	(Optional) Clears flap statistics for all address family sessions.
ipv4	(Optional) Clears flap statistics for IPv4 address family sessions.
multicast	(Optional) Clears flap statistics for multicast address family sessions.
mdt	(Optional) Clears flap statistics for multicast distribution tree (MDT) address family sessions.
unicast	(Optional) Clears flap statistics for unicast address family sessions.
ipv6	(Optional) Clears flap statistics for IPv6 address family sessions.
vpnv4	(Optional) Clears flap statistics for Virtual Private Network Version 4 (VPNv4) address family sessions.
vpnv6	(Optional) Clears flap statistics for Virtual Private Network Version 6 (VPNv6) address family sessions.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.0	This command was introduced.
12.0(22)S	The **vpnv4** and **ipv4** keywords were added.
12.0(29)S	The **mdt** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	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 **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

The **clear ip bgp flap-statistics** command is used to clear the accumulated penalty for routes that are received on a router that has BGP dampening enabled. If no arguments or keywords are specified, flap statistics are cleared for all routes. Flap statistics are also cleared when the peer is stable for the half-life time period.

Examples

In the following example, all of the flap statistics are cleared for paths that pass filter list 3:

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

In the following example, all of the flap statistics are cleared for the paths to the BGP neighbor at 10.2.1.3:

```
Router# clear ip bgp 10.2.1.3 flap-statistics
```

In the following example, all of the flap statistics are cleared for the paths to the BGP neighbor at 10.2.1.3 under IPv4 multicast address family:

```
Router# clear ip bgp 10.2.1.3 ipv4 multicast flap-statistics
```

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes various BGP route dampening factors.
clear ip bgp dampening	Clears BGP route dampening information and to unsuppress suppressed routes.
set dampening	Sets set BGP route dampening parameters in a route map.
show ip bgp dampened-paths	Displays BGP dampened routes.

clear ip bgp in prefix-filter

The **in** and **prefix-filter** keywords for the **clear ip bgp** command are no longer documented as a separate command.

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

clear ip bgp ipv4

To reset Border Gateway Protocol (BGP) connections using hard or soft reconfiguration for IPv4 address family sessions, use the **clear ip bgp ipv4** command in privileged EXEC mode.

clear ip bgp [**vrf** *vrf-name*] **ipv4** {**multicast** | **mdt** | **unicast**} *autonomous-system-number* [**in** [**prefix-filter**] | **out** | **slow** | **soft** [**in** [**prefix-filter**] | **out** | **slow**]]

Syntax Description

vrf	(Optional) Specifies an instance of a routing table.
vrf-name	(Optional) Name of the Virtual Private Network (VPN) routing and forwarding (VRF) table to use for storing data.
multicast	Resets multicast address family sessions.
mdt	Resets multicast distribution tree (MDT) address family sessions.
unicast	Resets unicast address family sessions.
autonomous-system-number	Resets BGP peers with the specified autonomous system number. Number in the range from 1 to 65535. • In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, 4-byte autonomous system numbers are supported in the range from 65536 to 4294967295 in asplain notation and in the range from 1.0 to 65535.65535 in asdot notation. • In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, 4-byte autonomous system numbers are supported in the range from 1.0 to 65535.65535 in asdot notation only. For more details about autonomous system number formats, see the **router bgp** command.
in	(Optional) Initiates inbound reconfiguration. If neither the **in** keyword nor the **out** keyword is specified, both inbound and outbound sessions are reset.
prefix-filter	(Optional) Clears the existing outbound route filter (ORF) prefix list to trigger a new route refresh or soft reconfiguration, which updates the ORF prefix list.
out	(Optional) Initiates outbound reconfiguration. If neither the **in** keyword nor the **out** keyword is specified, both inbound and outbound sessions are reset.
slow	(Optional) Clears slow-peer status forcefully and moves it to original update group.
soft	(Optional) Initiates a soft reset. Does not tear down the session.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.0(29)S	The **mdt** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX.
12.4(20)T	This command was modified. The **mdt** keyword was added.
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.
15.1(2)T	This command was modified. The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

The **clear ip bgp ipv4** command can be used to initiate a hard reset or soft reconfiguration. A hard reset tears down and rebuilds the specified peering sessions and rebuilds the BGP routing tables. A soft reconfiguration uses stored prefix information to reconfigure and activate BGP routing tables without tearing down existing peering sessions. Soft reconfiguration uses stored update information, at the cost of additional memory for storing the updates, to allow you to apply new BGP policy without disrupting the network. Soft reconfiguration can be configured for inbound or outbound sessions.

Generating Updates from Stored Information

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

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

Use this command whenever any of the following changes occur:

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

Dynamic Inbound Soft Reset

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

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

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

If all BGP routers support the route refresh capability, use the **clear ip bgp ipv4** command with the **in** keyword. You need not use the **soft** keyword, because soft reset is automatically assumed when the route refresh capability is supported.

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

Examples

In the following example, a soft reconfiguration is initiated for the inbound sessions for BGP neighbors in IPv4 unicast address family sessions in autonomous system 65400, and the outbound session is unaffected:

```
Router# clear ip bgp ipv4 unicast 65400 soft in
```

In the following example, the route refresh capability is enabled on the IPv4 multicast address family BGP neighbors in autonomous system 65000, a soft reconfiguration is initiated for all inbound sessions with the IPv4 multicast address family neighbors, and the outbound session is unaffected:

```
Router# clear ip bgp ipv4 multicast 65000 in
```

In the following example, a hard reset is initiated for all BGP neighbor in IPv4 MDT address family sessions in the autonomous system numbered 65400:

```
Router# clear ip bgp ipv4 mdt 65400
```

In the following example, a hard reset is initiated for BGP neighbors in IPv4 unicast address family sessions in the 4-byte autonomous system numbered 65538 in asplain notation. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, or a later release.

```
Router# clear ip bgp ipv4 unicast 65538
```

In the following example, a hard reset is initiated for BGP neighbors in IPv4 unicast address family sessions in the 4-byte autonomous system numbered 1.2 in asdot notation. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(32)S12, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, 12.4(24)T, and Cisco IOS XE Release 2.3, or a later release.

```
Router# clear ip bgp ipv4 unicast 1.2
```

Related Commands

Command	Description
neighbor soft-reconfiguration	Configures the Cisco IOS software to start storing updates.
router bgp	Configures the BGP routing process.
show ip bgp ipv4	Displays entries in the IPv4 BGP routing table.
show ip bgp neighbors	Displays information about BGP and TCP connections to neighbors.

clear ip bgp ipv6

To reset Border Gateway Protocol (BGP) connections using hard or soft reconfiguration for IPv6 address family sessions, use the **clear ip bgp ipv6** command in privileged EXEC mode.

clear ip bgp [**vrf** *vrf-name*] **ipv6** {**multicast** | **unicast**} *autonomous-system-number* [**in** [**prefix-filter**] | **out** | **slow** | **soft** [**in** [**prefix-filter**] | **out** | **slow**]]

Syntax Description

vrf	(Optional) Specifies an instance of a routing table.
vrf-name	(Optional) Name of the Virtual Private Network (VPN) routing and forwarding (VRF) table to use for storing data.
multicast	(Optional) Specifies the reset of multicast address family sessions.
unicast	(Optional) Specifies the reset of unicast address family sessions.
autonomous-system-number	Specifies that sessions with BGP peers in the specified autonomous system will be reset. Number in the range from 1 to 65535. • In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, 4-byte autonomous system numbers are supported in the range from 65536 to 4294967295 in asplain notation and in the range from 1.0 to 65535.65535 in asdot notation. • In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, 4-byte autonomous system numbers are supported in the range from 1.0 to 65535.65535 in asdot notation only. For more details about autonomous system number formats, see the **router bgp** command.
in	(Optional) Initiates inbound reconfiguration. If neither the **in** nor **out** keywords are specified, both inbound and outbound sessions are reset.
prefix-filter	(Optional) Clears the existing outbound route filter (ORF) prefix list to trigger a new route refresh or soft reconfiguration, which updates the ORF prefix list.
out	(Optional) Initiates inbound or outbound reconfiguration. If neither the **in** nor **out** keywords are specified, both inbound and outbound sessions are reset.
slow	(Optional) Clears slow-peer status forcefully and moves it to original update group.
soft	(Optional) Initiates a soft reset. Does not tear down the session.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX.
12.0(32)S12	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(24)T	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.3	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SXI1	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
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.
15.1(2)T	This command was modified. The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

The **clear ip bgp ipv6** command can be used to initiate a hard reset or soft reconfiguration of IPv6 address family sessions. A hard reset tears down and rebuilds the specified peering sessions and rebuilds the BGP routing tables. A soft reconfiguration uses stored prefix information to reconfigure and activate BGP routing tables without tearing down existing peering sessions. Soft reconfiguration uses stored update information, at the cost of additional memory for storing the updates, to allow you to apply new BGP policy without disrupting the network. Soft reconfiguration can be configured for inbound or outbound sessions.

Generating Updates from Stored Information

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

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

Use this command whenever any of the following changes occur:

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

- Changes to BGP-related distribution lists
- Changes to BGP-related route maps

Dynamic Inbound Soft Reset

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

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

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

If all BGP routers support the route refresh capability, use the **clear ip bgp ipv6** command with the **in** keyword. You need not use the **soft** keyword, because soft reset is automatically assumed when the route refresh capability is supported.

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

Examples

In the following example, a soft reconfiguration is initiated for the inbound sessions for BGP neighbors in IPv6 unicast address family sessions, and the outbound session is unaffected:

```
Router# clear ip bgp ipv6 unicast soft in
```

In the following example, the route refresh capability is enabled on the IPv6 multicast address family BGP neighbors and a soft reconfiguration is initiated for all inbound session with the IPv6 multicast address family neighbors, and the outbound session is unaffected:

```
Router# clear ip bgp ipv6 multicast in
```

In the following example, a hard reset is initiated for neighbor sessions with all IPv6 unicast address family routers in the autonomous system numbered 35400:

```
Router# clear ip bgp ipv6 unicast 35400
```

In the following example, a hard reset is initiated for BGP neighbors in IPv6 unicast address family sessions in the 4-byte autonomous system numbered 65538 in asplain notation. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, or a later release.

```
Router# clear ip bgp ipv6 unicast 65538
```

In the following example, a hard reset is initiated for BGP neighbors in IPv6 unicast address family sessions in the 4-byte autonomous system numbered 1.2 in asdot notation. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(32)S12, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, 12.4(24)T, and Cisco IOS XE Release 2.3, or a later release.

```
Router# clear ip bgp ipv6 unicast 1.2
```

Related Commands

Command	Description
neighbor soft-reconfiguration	Configures the Cisco IOS software to start storing updates.
router bgp	Configures the BGP routing process.
show ip bgp neighbors	Displays information about BGP and TCP connections to neighbors.

clear ip bgp l2vpn

To reset Border Gateway Protocol (BGP) neighbor session information for Layer 2 Virtual Private Network (L2VPN) address family, use the **clear ip bgp l2vpn** command in privileged EXEC mode.

clear ip bgp [**vrf** *vrf-name*] **l2vpn vpls** {*autonomous-system-number* | **peer-group** *peer-group-name* | **update-group** [*number* | *ip-address*]} [**in** [**prefix-filter**] | **out** | **slow** | **soft** [**in** [**prefix-filter**] | **out** | **slow**]]

Syntax Description

vrf	(Optional) Specifies an instance of a routing table.
vrf-name	(Optional) Name of the Virtual Private Network (VPN) routing and forwarding (VRF) table to use for storing data.
vpls	Specifies that Virtual Private LAN Service (VPLS) subsequent address family identifier (SAFI) information will be cleared.
autonomous-system-number	Autonomous system number in which peers are reset.
peer-group *peer-group-name*	Clears peer group information for the peer group specified with the *peer-group-name* argument.
update-group	Clears update group session information.
number	(Optional) Clears update-group session information for the specified update group number.
ip-address	(Optional) Clears update-group session information for the peer specified with the *ip-address* argument.
in	(Optional) Initiates inbound reconfiguration. If neither the **in** keyword nor **out** keyword is specified, both inbound and outbound sessions are reset.
prefix-filter	(Optional) Clears the inbound prefix filter.
out	(Optional) Initiates outbound reconfiguration. If neither the **in** keyword nor **out** keyword is specified, both inbound and outbound sessions are reset.
slow	(Optional) Clears slow-peer status forcefully and moves it to original update group.
soft	(Optional) Initiates a soft reset. Does not tear down the session.

Command Default

If no arguments or keywords are specified, all BGP L2VPN VPLS neighbor session information is cleared.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
Cisco IOS XE Release 2.4	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.

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.
15.1(2)T	This command was modified. The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

The **clear ip bgp l2vpn** command clears BGP session information for the L2VPN address family and VPLS SAFI. This command can be used to initiate a hard reset or soft reconfiguration. A hard reset tears down and rebuilds the specified peering sessions and rebuilds the BGP routing tables. A soft reconfiguration uses stored prefix information to reconfigure and activate BGP routing tables without tearing down existing peering sessions. Soft reconfiguration uses stored update information, at the cost of additional memory for storing the updates, to allow you to apply new BGP policy without disrupting the network. Soft reconfiguration can be configured for inbound or outbound sessions.

Generating Updates from Stored Information

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

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

Use the **clear ip bgp l2vpn** command whenever any of the following changes occur:

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

Dynamic Inbound Soft Reset

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

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

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

If all BGP routers support the route refresh capability, use the **clear ip bgp l2vpn vpls** {*autonomous-system-number* | **peer-group** *peer-group-name* | **update-group** [*number* | *ip-address*]} **in** command. You need not use the **soft** keyword, because soft reset is automatically assumed when the route refresh capability is supported.

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

Examples

The following example configures soft reconfiguration for the inbound session with BGP L2VPN peers in the 45000 autonomous system. The outbound session is unaffected:

```
Router# clear ip bgp l2vpn vpls 45000 soft in
```

Related Commands

Command	Description
address-family l2vpn	Enters address family configuration mode to configure a routing session using L2VPN endpoint provisioning information.
neighbor soft-reconfiguration	Configures the Cisco IOS software to start storing updates.

clear ip bgp peer-group

To reset Border Gateway Protocol (BGP) connections using hard or soft reconfiguration for all the members of a BGP peer group, use the **clear ip bgp peer-group** command in privileged EXEC mode.

Syntax Without Address Family Syntax

clear ip bgp [**vrf** *vrf-name*] **peer-group** *peer-group-name* [**in** [**prefix-filter**]] [**out**] [**soft** [**in** [**prefix-filter**] | **out**]]

Syntax With Address Family Syntax

clear ip bgp [**vrf** *vrf-name*] [**all** | **ipv4** {**multicast** | **mdt** | **unicast**} | **ipv6** {**multicast** | **unicast**} | **vpnv4 unicast** | **vpnv6 unicast**] **peer-group** *peer-group-name* [**in** [**prefix-filter**]] [**out**] [**soft** [**in** [**prefix-filter**] | **out**]]

Syntax Description

vrf	(Optional) Specifies an instance of a routing table.
vrf-name	(Optional) Name of the Virtual Private Network (VPN) routing and forwarding (VRF) table to use for storing data.
peer-group-name	Peer group name.
in	(Optional) Initiates inbound reconfiguration. If neither the **in** keyword nor the **out** keyword is specified, both inbound and outbound sessions are reset.
prefix-filter	(Optional) Clears the existing outbound route filter (ORF) prefix list to trigger a new route refresh or soft reconfiguration, which updates the ORF prefix list.
out	(Optional) Initiates outbound reconfiguration. If neither the **in** keyword nor the **out** keyword is specified, both inbound and outbound sessions are reset.
soft	(Optional) Initiates a soft reset. Does not tear down the session.
all	(Optional) Specifies the reset of peer group members in all address families.
ipv4	(Optional) Specifies the reset of peer group members in IPv4 address family sessions.
multicast	(Optional) Specifies the reset of peer group members in multicast address family sessions.
mdt	(Optional) Specifies the reset of peer group members in multicast distribution tree (MDT) address family sessions.
unicast	(Optional) Specifies the reset of peer group members in unicast address family sessions.
ipv6	(Optional) Specifies the reset of peer group members in IPv6 address family sessions.
vpnv4	(Optional) Specifies the reset of peer group members in Virtual Private Network Version 4 (VPNv4) address family sessions.
vpnv6	(Optional) Specifies the reset of peer group members in Virtual Private Network Version 6 (VPNv6) address family sessions.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.0	This command was introduced.
12.0(2)S	This command was integrated into Cisco IOS Release 12.0(2)S, and dynamic inbound soft reset capability was added.
12.0(7)T	The dynamic inbound soft reset capability was integrated into Cisco IOS Release 12.0(7)T.
12.0(22)S	The **vpnv4** and **ipv4** keywords were added.
12.0(29)S	The **mdt** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
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 **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

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

Generating Updates from Stored Information

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

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

Use this command whenever any of the following changes occur:

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

Dynamic Inbound Soft Reset

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

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

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

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

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

Examples

In the following example, all members of the BGP peer group named INTERNAL are reset:

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

In the following example, members of the peer group named EXTERNAL in IPv4 multicast address family sessions are reset:

```
Router# clear ip bgp ipv4 multicast peer-group EXTERNAL
```

In the following example, a soft reconfiguration is initiated for the inbound session with members of the peer group INTERNAL, and the outbound session is unaffected:

```
Router# clear ip bgp peer-group INTERNAL soft in
```

Related Commands

Command	Description
clear ip bgp	Resets a BGP connection or session.
neighbor peer-group (assigning members)	Configures a BGP neighbor to be a member of a peer group.
neighbor soft-reconfiguration	Configures the Cisco IOS software to start storing updates.
show ip bgp neighbors	Displays information about BGP and TCP connections to neighbors.

clear ip bgp table-map

To refresh table-map configuration information in the Border Gateway Protocol (BGP) routing table, use the **clear ip bgp table-map** command in privileged EXEC mode.

Syntax Without Address Family Syntax

clear ip bgp [**vrf** *vrf-name*] **table-map**

Syntax With Address Family Syntax

clear ip bgp [**vrf** *vrf-name*] [**ipv4** {**multicast** | **unicast**} | **vpnv4 unicast**] **table-map**

Syntax Description

vrf	(Optional) Specifies an instance of a routing table.
vrf-name	(Optional) Name of the Virtual Private Network (VPN) routing and forwarding (VRF) table to use for storing data.
ipv4	(Optional) Refreshes table-map configuration information for IPv4 address family sessions.
multicast	(Optional) Refreshes table-map configuration information for multicast address family sessions.
unicast	(Optional) Refreshes table-map configuration information for unicast address family sessions.
vpnv4	(Optional) Refreshes table-map configuration information for Virtual Private Network Version 4 (VPNv4) address family sessions.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(14)S	This command was introduced.
12.0(21)S	This command was integrated into Cisco IOS Release 12.0(21)S.
12.0(22)S	The **vpnv4** and **ipv4** keywords were added.
12.1(13)E	This command was integrated into Cisco IOS Release 12.1(13)E.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)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.
15.1(2)T	This command was modified. The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

The **clear ip bgp table-map** command is used to clear or refresh table-map configuration information in BGP routing tables. This command can be used to clear traffic-index information configured with the BGP Policy Accounting feature.

Examples

In the following example, a table map is configured and a traffic index is set. The new policy is applied after the **clear ip bgp table-map** command is entered.

```
Router(config)# route-map SET_BUCKET permit 10
Router(config-route-map)# match community 1
Router(config-route-map)# set traffic-index 2
Router(config-route-map)# exit
Router(config)# router bgp 50000
Router(config-router)# address-family ipv4
Router(config-router-af)# table-map SET_BUCKET
Router(config-router-af)# end
Router# clear ip bgp table-map
```

The following example clears the table map for IPv4 unicast peering sessions:

```
Router# clear ip bgp ipv4 unicast table-map
```

Related Commands

Command	Description
bgp-policy	Enables BGP policy accounting or policy propagation on an interface.
table-map	Modifies metrics and tag values when the IP routing table is updated with BGP learned routes.

clear ip bgp update-group

To reset Border Gateway Protocol (BGP) connections for all the members of a BGP update group, use the **clear ip bgp update-group** command in privileged EXEC mode.

Syntax Without Address Family Syntax

clear ip bgp [**vrf** *vrf-name*] **update-group** [*index-group* | *neighbor-address*]

Syntax With Address Family Syntax

clear ip bgp [**vrf** *vrf-name*] [**all** | **ipv4** {**multicast** | **mdt** | **unicast**} | **ipv6** {**multicast** | **unicast**} | **vpnv4 unicast** | **vpnv6 unicast**] **update-group** [*index-group* | *neighbor-address*]

Syntax Description

vrf	(Optional) Specifies an instance of a routing table.
vrf-name	(Optional) Name of the Virtual Private Network (VPN) routing and forwarding (VRF) table to use for storing data.
index-group	(Optional) Specifies that the update group with the specified index number will be reset. The range of update group index numbers is from 1 to 4294967295.
neighbor-address	(Optional) Specifies the IP address of a single peer that will be reset. The value for this argument can be an IPv4 or IPv6 address.
all	(Optional) Specifies the reset of update group members in all address families.
ipv4	(Optional) Specifies the reset of update group members in IPv4 address family sessions.
multicast	(Optional) Specifies the reset of update group members in multicast address family sessions.
mdt	(Optional) Specifies the reset of update group members in multicast distribution tree (MDT) address family sessions.
unicast	(Optional) Specifies the reset of update group members in unicast address family sessions.
ipv6	(Optional) Specifies the reset of update group members in IPv6 address family sessions.
vpnv4	(Optional) Specifies the reset of update group members in Virtual Private Network Version 4 (VPNv4) address family sessions.
vpnv6	(Optional) Specifies the reset of update group members in Virtual Private Network Version 6 (VPNv6) address family sessions.

Command Modes

Privileged EXEC (#)

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.

Release	Modification
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.0(29)S	The **mdt** keyword was added.
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.
12.2SX	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 **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

The **clear ip bgp update-group** command is used to clear BGP update group member sessions. If no keywords or arguments are specified, entering this command will recalculate all update groups. Specific index numbers for update groups and information about update-group membership is displayed in the output of the **show ip bgp update-group** and **debug ip bgp groups** commands.

When a change to outbound policy occurs, the BGP routing process will automatically recalculate update-group memberships and apply changes by triggering an outbound soft reset after a 1-minute timer expires. This behavior is designed to provide the network operator with time to change the configuration before the soft reset is initiated. You can immediately initiate the outbound soft reset before the timer expires by entering the **clear ip bgp** *ip-address* **soft out** command or immediately initiate a hard reset by entering the **clear ip bgp** *ip-address* command.

Note In Cisco IOS Release 12.0(25)S, 12.3(2)T, and prior releases, the update group recalculation delay timer is set to 3 minutes.

Examples

In the following example, the membership of the 10.0.0.1 peer is cleared from an update group:

```
Router# clear ip bgp update-group 10.0.0.1
```

In the following example, update-group information for all peers in the index 1 update group is cleared:

```
Router# clear ip bgp update-group 1
```

In the following example, update-group information for all MDT address family session peers in the index 6 update group is cleared:

```
Router# clear ip bgp ipv4 mdt update-group 6
```

Related Commands

Command	Description
clear ip bgp	Resets a BGP connection or session.
debug ip bgp groups	Displays information related to the processing of BGP update groups.
show ip bgp replication	Displays BGP update-group replication statistics.
show ip bgp update-group	Displays information about BGP update groups.

clear ip bgp vpnv4

To reset Border Gateway Protocol (BGP) connections using hard or soft reconfiguration for IPv4 Virtual Private Network (VPNv4) address family sessions, use the **clear ip bgp vpnv4** command in privileged EXEC mode.

clear ip bgp [**vrf** *vrf-name*] **vpnv4 unicast** *autonomous-system-number* [**in** [**prefix-filter**]] [**out**] [**slow**] [**soft** [**in** [**prefix-filter**] | **out** | **slow**]]

Syntax Description

vrf	(Optional) Specifies an instance of a routing table.
vrf-name	(Optional) Name of the Virtual Private Network (VPN) routing and forwarding (VRF) table to use for storing data.
unicast	Specifies the reset of unicast address family sessions.
autonomous-system-number	Specifies that sessions with BGP peers in the specified autonomous system will be reset. Number in the range from 1 to 65535. • In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, 4-byte autonomous system numbers are supported in the range from 65536 to 4294967295 in asplain notation and in the range from 1.0 to 65535.65535 in asdot notation. • In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, 4-byte autonomous system numbers are supported in the range from 1.0 to 65535.65535 in asdot notation only. For more details about autonomous system number formats, see the **router bgp** command.
in	(Optional) Initiates inbound reconfiguration. If neither the **in** nor **out** keywords are specified, both inbound and outbound sessions are reset.
prefix-filter	(Optional) Clears the existing outbound route filter (ORF) prefix list to trigger a new route refresh or soft reconfiguration, which updates the ORF prefix list.
out	(Optional) Initiates inbound or outbound reconfiguration. If neither the **in** nor **out** keywords are specified, both inbound and outbound sessions are reset.
slow	(Optional) Clears slow-peer status forcefully and moves it to original update group.
soft	(Optional) Initiates a soft reset. Does not tear down the session.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
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.
15.1(2)T	This command was modified. The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

The **clear ip bgp vpnv4** command can be used to initiate a hard reset or soft reconfiguration of VPNv4 address family sessions. A hard reset tears down and rebuilds the specified peering sessions and rebuilds the BGP routing tables. A soft reconfiguration uses stored prefix information to reconfigure and activate BGP routing tables without tearing down existing peering sessions. Soft reconfiguration uses stored update information, at the cost of additional memory for storing the updates, to allow you to apply new BGP policy without disrupting the network. Soft reconfiguration can be configured for inbound or outbound sessions.

Generating Updates from Stored Information

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

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

Use this command whenever any of the following changes occur:

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

Dynamic Inbound Soft Reset

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

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

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

If all BGP routers support the route refresh capability, use the **clear ip bgp vpnv4** command with the **in** keyword. You need not use the **soft** keyword, because soft reset is automatically assumed when the route refresh capability is supported.

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

Examples

In the following example, a soft reconfiguration is initiated for the inbound sessions for BGP neighbors in VPNv4 unicast address family sessions, and the outbound session is unaffected:

```
Router# clear ip bgp vpnv4 unicast soft in
```

In the following example, the route refresh capability is enabled on theVPNv4 unicast address family BGP neighbors and a soft reconfiguration is initiated for all inbound session with the VPNv4 multicast address family neighbors, and the outbound session is unaffected:

```
Router# clear ip bgp vpnv4 unicast in
```

In the following example, a hard reset is initiated for neighbor sessions with all VPNv4 unicast address family routers in the autonomous system numbered 35700:

```
Router# clear ip bgp vpnv4 unicast 35700
```

In the following example, a hard reset is initiated for BGP neighbors in IPv4 unicast address family sessions in the 4-byte autonomous system numbered 65538 in asplain notation. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, or a later release.

```
Router# clear ip bgp vpnv4 unicast 65538
```

In the following example, a hard reset is initiated for BGP neighbors in IPv4 unicast address family sessions in the 4-byte autonomous system numbered 1.2 in asdot notation. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(32)S12, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, 12.4(24)T, and Cisco IOS XE Release 2.3, or a later release.

```
Router# clear ip bgp vpnv4 unicast 1.2
```

Related Commands

Command	Description
neighbor soft-reconfiguration	Configures the Cisco IOS software to start storing updates.
show ip bgp neighbors	Displays information about BGP and TCP connections to neighbors.

clear ip bgp vpnv4 unicast dampening

To reset Border Gateway Protocol (BGP) route flap dampening for a particular IPv4 Virtual Private Network version 4 (VPNv4) address family prefix, use the **clear ip bgp vpnv4 unicast dampening** command in privileged EXEC mode.

clear ip bgp vpnv4 unicast dampening rd *route-distinguisher* [*network-address* [*network-mask*]]

Syntax Description

rd *route-distinguisher*	(Optional) VPN route distinquisher (RD) is either an autonomous system number (ASN)-relative RD, in which case it is composed of an autonomous system number and an arbitrary number, or it is an IP-address-relative RD, in which case it is composed of an IP address and an arbitrary number. You can enter a *route-distinguisher* in either of these formats: • 16-bit autonomous system number: your 32-bit number. For example, 10:1. • 32-bit IP address: your 16-bit number. For example, 192.168.122.15:1.
network-address	(Optional) IPv4 address for which the flap statistics are cleared.
network-mask	(Optional) IPv4 network mask.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

You can use the **clear ip bgp vpnv4 unicast dampening** command to clear stored route dampening information for the VPNv4 address family. If you specify a route-distinguisher in the command, the command clears all the prefixes that contain the particular route-distinguisher. If you specify a VPNv4 address in the command, the command clears the route dampening information for that particular network address.

Examples

The following example shows how to reset the flap dampening for a particular VPNv4 prefix:

```
Router# clear ip bgp vpnv4 unicast dampening rd 10:1 192.168.2.1 255.255.255.0
```

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or configures BGP route dampening parameters.
clear ip bgp flap-statistics	Resets BGP route dampening flap-statistics.

Command	Description
set dampening	Sets route dampening parameters in a route map.
show ip bgp dampened-paths	Displays BGP dampened routes.

clear ip bgp vpnv6

To reset Border Gateway Protocol (BGP) connections using hard or soft reconfiguration for IPv6 Virtual Private Network (VPNv6) address family sessions, use the **clear ip bgp vpnv6** command in privileged EXEC mode.

clear ip bgp vpnv6 unicast *autonomous-system-number* [**in** [**prefix-filter**]] [**out**] [**slow**] [**soft** [**in** [**prefix-filter**] | **out** | **slow**]]

Syntax Description

unicast	Specifies the reset of unicast address family sessions.
autonomous-system-number	Specifies that sessions with BGP peers in the specified autonomous system will be reset. Number in the range from 1 to 65535. • In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, 4-byte autonomous system numbers are supported in the range from 65536 to 4294967295 in asplain notation and in the range from 1.0 to 65535.65535 in asdot notation. • In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, 4-byte autonomous system numbers are supported in the range from 1.0 to 65535.65535 in asdot notation only. For more details about autonomous system number formats, see the **router bgp** command.
in	(Optional) Initiates inbound reconfiguration. If neither the **in** nor **out** keywords are specified, both inbound and outbound sessions are reset.
prefix-filter	(Optional) Clears the existing outbound route filter (ORF) prefix list to trigger a new route refresh or soft reconfiguration, which updates the ORF prefix list.
out	(Optional) Initiates inbound or outbound reconfiguration. If neither the **in** nor **out** keywords are specified, both inbound and outbound sessions are reset.
slow	(Optional) Clears slow-peer status forcefully and moves it to original update group.
soft	(Optional) Initiates a soft reset. Does not tear down the session.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)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.

Release	Modification
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 **clear ip bgp vpnv6** command can be used to initiate a hard reset or soft reconfiguration of VPNv6 address family sessions. A hard reset tears down and rebuilds the specified peering sessions and rebuilds the BGP routing tables. A soft reconfiguration uses stored prefix information to reconfigure and activate BGP routing tables without tearing down existing peering sessions. Soft reconfiguration uses stored update information, at the cost of additional memory for storing the updates, to allow you to apply new BGP policy without disrupting the network. Soft reconfiguration can be configured for inbound or outbound sessions.

Generating Updates from Stored Information

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

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

Use this command whenever any of the following changes occur:

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

Dynamic Inbound Soft Reset

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

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

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

If all BGP routers support the route refresh capability, use the **clear ip bgp vpnv6** command with the **in** keyword. You need not use the **soft** keyword, because soft reset is automatically assumed when the route refresh capability is supported.

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

Examples

In the following example, a soft reconfiguration is initiated for the inbound sessions for BGP neighbors in VPNv6 unicast address family sessions, and the outbound session is unaffected:

```
Router# clear ip bgp vpnv6 unicast soft in
```

In the following example, the route refresh capability is enabled on the VPNv6 unicast address family BGP neighbors and a soft reconfiguration is initiated for all inbound session with the IPv6 multicast address family neighbors, and the outbound session is unaffected:

```
Router# clear ip bgp vpnv6 unicast in
```

In the following example, a hard reset is initiated for neighbor sessions with all VPNv6 unicast address family routers in the autonomous system numbered 35700:

```
Router# clear ip bgp vpnv6 unicast 35700
```

In the following example, a hard reset is initiated for BGP neighbors in VPNv6 unicast address family sessions in the 4-byte autonomous system numbered 65538 in asplain notation. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, or a later release.

```
Router# clear ip bgp vpnv6 unicast 65538
```

In the following example, a hard reset is initiated for BGP neighbors in VPNv6 unicast address family sessions in the 4-byte autonomous system numbered 1.2 in asdot notation. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(32)S12, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, 12.4(24)T, and Cisco IOS XE Release 2.3, or a later release.

```
Router# clear ip bgp vpnv6 unicast 1.2
```

Related Commands

Command	Description
neighbor soft-reconfiguration	Configures the Cisco IOS software to start storing updates.
show ip bgp neighbors	Displays information about BGP and TCP connections to neighbors.

clear ip bgp vpnv6 unicast dampening

To reset Border Gateway Protocol (BGP) route flap dampening for a particular IPv6 Virtual Private Network version 6 (VPNv6) address family prefix, use the **clear ip bgp vpnv6 unicast dampening** command in privileged EXEC mode.

clear ip bgp vpnv6 unicast dampening [**rd** *route-distinguisher* [*network-address*]]

Syntax Description

rd *route-distinguisher*	(Optional) The VPN route distinquisher (RD) is either an autonomous system number (ASN)-relative RD, in which case it is composed of an autonomous system number and an arbitrary number, or it is an IP-address-relative RD, in which case it is composed of an IP address and an arbitrary number. You can enter a *route-distinguisher* in either of these formats: • 16-bit autonomous system number: your 32-bit number. For example, 10:1. • 32-bit IP address: your 16-bit number. For example, 192.168.122.15:1.
network-address	(Optional) VPNv6 address for which the flap statistics are cleared.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

You can use the **clear ip bgp vpnv6 unicast dampening** command to clear stored route dampening information for the VPNv6 address family. If you specify a route-distinguisher in the command, the command clears all the prefixes that contain the particular route-distinguisher. If you specify a VPNv6 address in the command, the command clears the route dampening information for that particular network address.

Examples

The following example shows how to reset the flap dampening for a particular VPNv6 prefix:

```
Router# clear ip bgp vpnv6 unicast dampening rd 1:0 2001:1000::0/64
```

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or configures BGP route dampening parameters.
clear ip bgp flap-statistics	Resets BGP route dampening flap-statistics.

Command	Description
set dampening	Sets route dampening parameters in a route map.
show ip bgp dampened-paths	Displays BGP dampened routes.

clear ip prefix-list

To reset IP prefix-list counters, use the **clear ip prefix-list** command in privileged EXEC mode.

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

Syntax Description

prefix-list-name	(Optional) Name of the prefix list from which the hit count is to be cleared.
network/length	(Optional) Network number and length (in bits) of the network mask. The slash mark must precede the bit length value.

Command Modes

Privileged EXEC

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 **clear ip prefix-list** command is used to clear prefix-list hit counters. The hit count is a value indicating the number of matches to a specific prefix list entry.

Examples

In the following example, the prefix-list counters are cleared for the prefix list named FIRST_LIST that matches the 10.0.0.0/8 prefix:

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

Related Commands

Command	Description
distribute-list in (IP)	Filters networks received in updates.
distribute-list out (IP)	Suppresses networks from being advertised in updates.
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.
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.
show ip bgp regexp	Displays information about a prefix list or prefix list entries.

continue

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

continue [*sequence-number*]

no continue

Syntax Description

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

Defaults

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

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

Command Modes

Route-map configuration (config-route-map)

Command History

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

Usage Guidelines

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

Route Map Operation Without Continue Clauses

A route map evaluates match clauses until a successful match occurs. After the match occurs, the route map stops evaluating match clauses and starts executing set clauses, in the order in which they were configured. If a successful match does not occur, the route map "falls through" and evaluates the next sequence number of the route map until all configured route-map entries have been evaluated or a successful match occurs. Each route-map sequence is tagged with a sequence number to identify the

entry. Route-map entries are evaluated in order starting with the lowest sequence number and ending with the highest sequence number. If the route map contains only set clauses, the set clauses will be executed automatically, and the route map will not evaluate any other route-map entries.

Route Map Operation With Continue Clauses

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

Match Operations With Continue Clauses

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

Set Operations With Continue Clauses

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

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

Examples

In the following example, continue clause configuration is shown.

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

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

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

```
Router(config)# route-map ROUTE-MAP-NAME permit 10
Router(config-route-map)# match ip address 1
Router(config-route-map)# match metric 10
Router(config-route-map)# set as-path prepend 10
Router(config-route-map)# continue 30
Router(config-route-map)# exit
Router(config)# route-map ROUTE-MAP-NAME permit 20
Router(config-route-map)# match ip address 2
Router(config-route-map)# match metric 20
Router(config-route-map)# set as-path prepend 10 10
Router(config-route-map)# exit
Router(config)# route-map ROUTE-MAP-NAME permit 30
Router(config-route-map)# set as-path prepend 10 10 10
Router(config-route-map)# continue
Router(config-route-map)# exit
Router(config)# route-map ROUTE-MAP-NAME permit 40
Router(config-route-map)# match community 10:1
Router(config-route-map)# set local-preference 104
Router(config-route-map)# exit
```

Related Commands

Command	Description
aggregate-address	Creates an aggregate entry in a BGP or multicast BGP database.
match as-path	Match BGP autonomous system path access lists.
match community	Matches a BGP community.
match extcommunity	Matches a BGP extended community.
match interface (IP)	Distributes routes that have their next hop out one of the interfaces specified.
match ip address	Distributes any routes that have a destination network number address permitted by a standard or extended access list, or performs policy routing on packets.
match ip next-hop	Redistributes any routes that have a next-hop router address passed by one of the access lists specified.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match length	Bases policy routing on the Level 3 length of a packet.
match metric (IP)	Redistributes routes with the metric specified.
match mpls-label	Redistributes routes that include MPLS labels if the routes meet the conditions specified in the route map.
match route-type (IP)	Redistributes routes of the specified type.
match tag	Redistributes routes in the routing table that match the specified tags.
neighbor default-originate	Allows a BGP speaker (the local router) to send the default route 0.0.0.0 to a neighbor for use as a default route.
neighbor route-map	Applies a route map to incoming or outgoing routes.
neighbor remote-as	Adds an entry to the BGP or multiprotocol BGP neighbor table.
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol to another, or enables policy routing.
set as-path	Modifies an autonomous system path for BGP routes.
set automatic-tag	Automatically computes the tag value in a route-map configuration.

Command	Description
set comm-list delete	Removes communities from the community attribute of an inbound or outbound update.
set community	Sets the BGP communities attribute.
set dampening	Sets the BGP route dampening factors.
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set extcommunity	Sets the BGP extended communities attribute.
set interface	Indicates where to output packets that pass a match clause of route map for policy routing.
set ip default next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing and for which the Cisco IOS software has no explicit route to a destination.
set ip default next-hop verify-availability	Configures a router to check the CDP database for the availability of an entry for the default next hop that is specified by the set ip default next-hop command.
set ip next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing.
set ip next-hop verify-availability	Configures policy routing to verify if the next hops of a route map are CDP neighbors before policy routing to those next hops.
set ip precedence	Sets the precedence value in the IP header.
set level (IP)	Indicates where to import routes.
set local-preference	Specifies a preference value for the autonomous system path.
set mpls-label	Enables a route to be distributed with an MPLS label if the route matches the conditions specified in the route map.
set next-hop	Specifies the address of the next hop.
set nlri	This command was replaced by the address-family ipv4 and address-family vpnv4 commands.
set origin (BGP)	Sets the BGP origin code.
set qos-group	Sets a group ID that can be used later to classify packets.
set tag (IP)	Sets the value of the destination routing protocol.
set traffic-index	Defines where to output packets that pass a match clause of a route map for BGP policy accounting.
set weight	Specifies the BGP weight for the routing table.
show ip bgp	Displays entries in the BGP routing table.
show route-map	Displays all route maps configured or only the one specified.

debug ip bgp igp-metric ignore

To display information related to the system ignoring the Interior Gateway Protocol (IGP) metric during best path selection, use the **debug ip bgp igp-metric ignore** command in privileged EXEC mode. To disable such debugging output, use the **no** form of the command.

debug ip bgp igp-metric ignore

no debug ip bgp igp-metric ignore

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

You might use this command if the path you expected to be chosen as the best path at the shadow RR was not chosen as such. That could be because the **bgp bestpath igp-metric ignore** command makes the best path algorithm choose the same best path as the primary RR if they are not co-located.

Examples

The following example turns on debugging of events related to the system ignoring the IGP metric during bestpath selection:

```
Router# debug ip bgp igp-metric ignore
```

Related Commands

Command	Description
bgp bestpath igp-metric ignore	Specifies that the system ignore the Interior Gateway Protocol (IGP) metric during best path selection.

debug ip bgp route-server

To turn on debugging for a BGP route server, use the **debug ip bgp route-server** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ip bgp route-server {**client** | **context** | **event** | **import** | **policy**} [**detail**]

no debug ip bgp route-server {**client** | **context** | **event** | **import** | **policy**} [**detail**]

Syntax Description

client	Displays information about BGP route server clients.
context	Displays information about BGP route server contexts.
event	Displays information about route server events, such as importing into the virtual RS table.
import	Displays information about BGP route server import maps.
policy	Displays information about the policy path process.
detail	(Optional) Displays detailed debugging information.

Command Modes

Privilaged EXEC (#)

Command History

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

Usage Guidelines

Use this command to turn on debugging of a BGP router server.

Caution The **detail** keyword is used for complex issues and should only be turned on when you are debugging with a Cisco representative.

Examples

In the following example, BGP route server client debugging is turned on:

```
Router# debug ip bgp route-server client
```

Related Commands

Command	Description
import-map	Configures flexible policy handling by a BGP route server.
neighbor route-server-client	Specifies on a BGP route server that a neighbor is a route server client.
route-server-context	Creates a route-server context in order to provide flexible policy handling for a BGP route server.

default-information originate (BGP)

To configure a Border Gateway Protocol (BGP) routing process to distribute a default route (network 0.0.0.0), use the **default-information originate** command in address family or router configuration mode. To disable the advertisement of a default route, use the **no** form of this command.

default-information originate

no default-information originate

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Address family configuration
Router configuration

Command History

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

Usage Guidelines

The **default-information originate** command is used to configure a BGP routing process to advertise a default route (network 0.0.0.0). A redistribution statement must also be configured to complete this configuration or the default route will not be advertised.

The configuration of the **default-information originate** command in BGP is similar to the configuration of the **network (BGP)** command. The **default-information originate** command, however, requires explicit redistribution of the route 0.0.0.0. The **network** command requires only that the route 0.0.0.0 is present in the Interior Gateway Protocol (IGP) routing table. For this reason, the **network** command is preferred.

Note The **default-information originate** command should not be configured with the **neighbor default-originate** command on the same router. You should configure one or the other.

Examples

In the following example, the router is configured to redistribute a default route from OSPF into the BGP routing process:

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

```
Router(config-router-af)# default-information originate
Router(config-router-af)# redistribute ospf 100
Router(config-router-af)# end
```

Related Commands

Command	Description
neighbor default-originate	Configures a BGP routing process to send a default route (network 0.0.0.0) to a neighbor.
network (BGP)net	Specifies the list of networks for the BGP routing process.
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.

default-metric (BGP)

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

default-metric *number*

no default-metric *number*

Syntax Description

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

Defaults

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

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

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

Command Modes

Address family configuration
Router configuration

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

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

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

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

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

BGP table version is 7, local router ID is 192.168.2.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 172.17.1.0/24    192.168.2.2                              0 65502 i
```

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

```
Router# show ip bgp neighbors 172.16.1.2 received-routes

BGP table version is 2, local router ID is 172.16.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
* i172.16.1.0/24    172.16.1.2               0    100      0 i
* i172.17.1.0/24    192.168.2.2            300    100      0 65502 i

Total number of prefixes 2
```

Related Commands

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

description (route server context)

To specify a description for a BGP route server context, use the **description** command in route server context configuration mode. To remove the description, use the **no** form of this command.

description *string*

no description

Syntax Description

string	Description of the route server context. The string can be up to 80 characters long.

Command Default

No description for a route server context exists.

Command Modes

Route server context configuration (config-router-rsctx)

Command History

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

Usage Guidelines

Create a route server context if you want your BGP route server to support customized, flexible policies. The routes needing flexible policy handling are selected for import into a route server context by an import map that you configure. The import map references a route map, where the actual policy is defined.

The **description** command allows an optional description of a route server context to remind you of the purpose of the context or policy, for example. This is more user-friendly and scannable than trying to interpret the route map commands when looking at a configuration file or **show** output.

Examples

In the following example, the description is a user-friendly way to see the purpose of the context, without having to interpret the import map and route map:

```
Router(config)# router bgp 65000
Router(config-router)# route-server-context only_AS27_context
Router(config-router-rsctx)# description Context references route map permitting only
routes with AS 27 in AS path.
```

Related Commands

Command	Description
import-map	Configures flexible policy handling by a BGP route server.
route-server-context	Creates a route-server context in order to provide flexible policy handling for a BGP route server.

distance bgp

To configure the administrative distance for BGP routes, use the **distance bgp** command in address family or router configuration mode. To return to the administrative distance to the default value, use the **no** form of this command.

distance bgp *external-distance internal-distance local-distance*

no distance bgp

Syntax Description

external-distance	Administrative distance for external BGP routes. Routes are external when learned from an external autonomous system. The range of values for this argument are from 1 to 255.
internal-distance	Administrative distance for internal BGP routes. Routes are internal when learned from peer in the local autonomous system. The range of values for this argument are from 1 to 255.
local-distance	Administrative distance for local BGP routes. Local routes are those networks listed with a **network** router configuration command, often as back doors, for the router or for the networks that is being redistributed from another process. The range of values for this argument are from 1 to 255.

Defaults

The following values are used if this command is not configured or if the no form is entered:

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

Routes with a distance of 255 are not installed in the routing table.

Command Modes

Address family configuration
Router configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(7)T	Address family configuration mode support was added.
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 **distance bgp** command is used to configure a rating of the trustworthiness of a routing information source, such as an individual router or a group of routers. Numerically, an administrative distance is a positive integer from 1 to 255. In general, the higher the value, the lower the trust rating. An administrative distance of 255 means the routing information source cannot be trusted at all and should

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

Caution Changing the administrative distance of internal BGP routes is considered dangerous and is not recommended. Improper configuration can introduce routing table inconsistencies and break routing.

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

Examples

In the following example, the external distance is set to 10, the internal distance is set to 50, and the local distance is set to 100:

```
Router(config)# router bgp 50000
Router(config-router)# address family ipv4 multicast
Router(config-router-af)# network 10.108.0.0
Router(config-router-af)# neighbor 192.168.6.6 remote-as 123
Router(config-router-af)# neighbor 172.16.1.1 remote-as 47
Router(config-router-af)# distance bgp 10 50 100
Router(config-router-af)# end
```

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.

distribute-list in (BGP)

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

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

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

Syntax Description

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

Defaults

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

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
11.2	The *acl-number* arguments was added.
12.0	The **prefix** keyword and *list-name* argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **distribute-list in** command is used to filter incoming BGP updates. An access list or prefix list must be defined prior to configuration of this command. Standard and expanded access lists are supported. IP prefix lists are used to filter based on the bit length of the prefix. An entire network, subnet, supernet, or single host route can be specified. Prefix list and access list configuration is mutually exclusive when configuring a distribute list. The session must be reset with the **clear ip bgp** command before the distribute list will take effect.

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

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

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

Examples

In the following example, a prefix list and distribute list are defined to configure the BGP routing process to accept traffic from only network 10.1.1.0/24, network 192.168.1.0, and network 10.108.0.0. An inbound route refresh is initiated to activate the distribute-list.

```
Router(config)# ip prefix-list RED permit 10.1.1.0/24
Router(config)# ip prefix-list RED permit 10.108.0.0/16
Router(config)# ip prefix-list RED permit 192.168.1.0/24
Router(config)# router bgp 50000
Router(config-router)# network 10.108.0.0
Router(config-router)# distribute-list prefix RED in
Router(config-router)# end
Router# clear ip bgp in
```

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

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

Related Commands

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

distribute-list out (BGP)

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

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

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

Syntax Description

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

Defaults

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

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
11.2	The *acl-number* argument was added.
12.0	The **prefix** keyword and *list-name* argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **distribute-list out** command is used to filter outbound BGP updates. An access list or prefix list must be defined prior to configuration of this command. Standard and expanded access lists are supported. IP prefix lists are used to filter based on the bit length of the prefix. An entire network, subnet, supernet, or single host route can be specified. Prefix list and access list configuration is mutually exclusive when configuring a distribute list. The session must be reset with the **clear ip bgp** command before the distribute list will take effect.

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

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

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

To suppress networks or routes from being received in inbound updates, use the **distribute-list in** command.

Examples

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

```
Router(config)# ip prefix-list BLUE permit 192.168.0.0/16
Router(config)# router bgp 50000
Router(config-router)# distribute-list prefix BLUE out
Router(config-router)# end
Router# clear ip bgp out
```

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

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

Related Commands

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

exit-peer-policy

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

exit-peer-policy

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Modes

Policy-template 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.

Examples

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

```
Router(config-router-ptmp)# exit-peer-policy
Router(config-router)#
```

Related Commands

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

exit-peer-session

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

exit-peer-session

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Session-template 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.

Examples

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

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

Related Commands

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

exit-route-server-context

To exit a route server context and return to router configuration mode, use the **exit-route-server-context** command in route server context configuration mode.

exit-route-server-context

Syntax Description

This command has no arguments or keywords.

Command Modes

Route server context configuration (config-router-rsctx)

Command History

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

Usage Guidelines

When you configure a BGP route server with a flexible policy, you create a route server context with an import map, which is when you might use the **exit-route-server-context** command. The **exit-route-server-context** command is one of the commands that will be displayed in system help if you enter a ? at the Router(config-router-rsctx)# prompt. However, the **exit** command performs the same function as the **exit-route-server-context** command.

Examples

In the following example, a route server context is created and the **exit-route-server-context** command is used to exit route server context configuration mode:

```
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
   !
Router(config)#
```

Related Commands

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

export map

To associate an export map with a VPN Routing and Forwarding (VRF) instance, use the **export map** command in IP VRF configuration or in VRF address family configuration mode. To remove the export map, use the **no** form of this command.

export map *route-map*

no export map *route-map*

Syntax Description

route-map	Specifies the route map to be used as an export map.

Command Default

No export maps are associated with a VRF instance.

Command Modes

IP VRF configuration (config-vrf)
VRF address family configuration (config-vrf-af)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

The **export map** command is used to associate a route map with the specified VRF. The export map is used to filter routes that are eligible for export out of a VRF, based on the route target extended community attributes of the route. Only one export route map can be configured for a VRF.

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

You can access the **export map** command by using the **ip vrf** global configuration command. You can also access the **export map** command by using the **vrf definition** global configuration command followed by the **address-family** VRF configuration command.

Examples

In the following example, an export is configured under the VRF and an access list and route map are configured to specify which prefixes are exported:

```
Router(config)# ip vrf RED
Router(config-vrf)# rd 1:1
Router(config-vrf)# export map BLUE
Router(config-vrf)# route-target import 2:1
```

```
Router(config-vrf)# exit
Router(config)# access-list 1 permit 192.168.0.0 0.0.255.255
Router(config)# route-map BLUE permit 10
Router(config-route-map)# match ip address 1
Router(config-route-map)# set extcommunity rt 2:1
Router(config-route-map)# end
```

Related Commands

Command	Description
address-family (VRF)	Selects an address family type for a VRF table and enters VRF address family configuration mode.
import map	Configures an import route map for a VRF.
ip extcommunity-list	Creates an extended community list for BGP and controls access to it.
ip vrf	Configures a VRF routing table.
route-target	Creates a route-target extended community for a VRF.
show ip vrf	Displays the set of defined VRFs and associated interfaces.
vrf definition	Configures a VRF routing table instance and enters VRF configuration mode.

ha-mode graceful-restart

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

ha-mode graceful-restart [**disable**]

no ha-mode graceful-restart [**disable**]

Syntax Description

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

Command Default

BGP graceful restart is disabled.

Command Modes

Peer session template configuration (config-router-stmp)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

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

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

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

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

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

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

Examples

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

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

Related Commands

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

import ipv4

To configure an import map to import IPv4 prefixes from the global routing table to a VRF table, use the **import ipv4** command in VRF configuration or in VRF address family configuration mode. To remove the import map, use the **no** form of this command.

import ipv4 {**unicast** | **multicast**} [*prefix-limit*] **map** *route-map*

no import ipv4 {**unicast** | **multicast**} [*prefix-limit*] **map** *route-map*

Syntax Description

unicast	Specifies IPv4 unicast prefixes to import.
multicast	Specifies IPv4 multicast prefixes to import.
prefix-limit	(Optional) Number of prefixes to import. The range is from 1 to 2147483647. Default is 1000.
map *route-map*	Specifies the route map to be used as an import route map for the VRF.

Command Default

No import map is configured.

Command Modes

VRF configuration (config-vrf)
VRF address family configuration (config-vrf-af)

Command History

Release	Modification
12.0(29)S	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)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.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

IP prefixes that are defined for import are processed through a match clause in a route map. The prefixes that pass through the route map are imported into the Virtual Private Network (VPN) routing/forwarding (VRF) instance. A maximum of five VRFs per router can be configured to import IPv4 prefixes from the global routing table. 1000 prefixes per VRF are imported by default. You can manually configure from 1 to 2,147,483,647 prefixes for each VRF. We recommend that you use caution if you manually configure the prefix import limit. Configuring the router to import too many prefixes can interrupt normal router operation. Only IPv4 unicast and multicast prefixes can be imported to a VRF with this feature. IPv4 prefixes imported into a VRF using this feature cannot be imported into a VPNv4 VRF.

You can access the **import ipv4** command by using the **ip vrf** global configuration command. You can also access the **import ipv4** command by using the **vrf definition** global configuration command followed by the **address-family** VRF configuration command.

No MPLS or Route Target Configuration Is Required

No MPLS or route target (import/export) configuration is required.

Import Behavior

Import actions are triggered when a new routing update is received or when routes are withdrawn. During the initial BGP update period, the import action is postponed to allow BGP to converge more quickly. Once BGP converges, incremental BGP updates are evaluated immediately and qualified prefixes are imported as they are received.

Examples

The following example, beginning in global configuration mode, imports all unicast prefixes from the 10.24.240.0/22 subnet into the VRF named GREEN. An IP prefix list is used to define the imported IPv4 prefixes. The route map is attached to the Ethernet interface 0, and unicast RPF verification for VRF GREEN is enabled.

```
ip prefix-list COLORADO permit 10.24.240.0/22
!
ip vrf GREEN
 rd 100:10
 import ipv4 unicast 1000 map UNICAST
 exit
route-map UNICAST permit 10
 match ip address prefix-list ACCOUNTING
 exit
interface Ethernet 0
 ip policy route-map UNICAST
 ip verify unicast vrf GREEN permit
 end
```

Related Commands

Command	Description
address-family (VRF)	Selects an address family type for a VRF table and enters VRF address family configuration mode.
ip verify unicast vrf	Enables Unicast Reverse Path Forwarding verification for the specified VRF.
ip vrf	Configures a VRF routing table.
rd	Creates routing and forwarding tables for a VRF.
show ip bgp	Displays entries in the BGP routing table.
show ip bgp vpnv4	Displays VPN address information from the BGP table.
show ip vrf	Displays the set of defined VRFs and associated interfaces.
vrf definition	Configures a VRF routing table instance and enters VRF configuration mode.

import path limit

To specify the maximum number of Border Gateway Protocol (BGP) paths, per VPN routing and forwarding (VRF) importing net, that can be imported from an exporting net, use the **import path limit** command in address family configuration mode. To reset the BGP path import limit to the default value, use the **no** form of this command.

import path limit *number-of-import-paths*

no import path limit *number-of-import-paths*

Syntax Description

number-of-import-paths	Maximum number of BGP paths, per importing net, that can be imported from an exporting net.

Command Default

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

Command Modes

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

Command History

Release	Modification
15.0(1)M	This command was introduced.
12.2(1st)SRE	This command was integrated into Cisco IOS Release 12.2(1st)SRE.
Cisco IOS XE 2.6	This command was integrated into Cisco IOS XE Release 2.6

Usage Guidelines

Use the **import path limit** command to control memory utilization when importing paths using the BGP Event-Based VPN Import feature. A maximum limit of the number of paths imported from an exporting net can be specified, per importing net. When a selection is made of paths to be imported from one or more exporting net, the first selection priority is a bestpath, the next selection priority is for multipaths, and the lowest selection priority is for nonmultipaths. The import path policy is set using the **import path selection** command.

The BGP Event-Based VPN Import feature introduces a modification to the existing BGP path import process. BGP Virtual Private Network (VPN) import provides importing functionality for BGP paths where BGP paths are imported from the BGP VPN table into a BGP virtual routing and forwarding (VRF) topology. In the existing path import process, when path updates occur, the import updates are processed during the next scan time which is a configurable interval of 5 to 15 seconds. The scan time adds a delay in the propagation of routes. The enhanced BGP path import is driven by events; when a BGP path changes, all of its imported copies are updated as soon as processing is available.

Using the BGP Event-Based VPN Import feature, convergence times are significantly reduced because provider edge (PE) routers can propagate VPN paths to customer edge (CE) routers without the scan time delay. Configuration changes such as adding imported route-targets to a VRF are not processed immediately, and are still handled during the 60-second periodic scanner pass.

Examples

The following example shows how to specify a maximum number of BGP paths to import from an exporting net for each importing net. Two BGP neighbors are configured in BGP router configuration mode and are activated in VPNv4 address family configuration mode. In IPv4 VRF address family configuration mode, the import path selection is set to all, and the number of import paths is set to 3.

```
Router(config)# router bgp 45000
Router(config-router)# neighbor 192.168.1.2 remote-as 40000
Router(config-router)# neighbor 192.168.3.2 remote-as 50000
Router(config-router)# address-family vpnv4
Router(config-router-af)# neighbor 192.168.1.2 activate
Router(config-router-af)# neighbor 192.168.3.2 activate
Router(config-router-af)# exit-address-family
Router(config-router)# address-family ipv4 vrf vrf-A
Router(config-router-af)# import path selection all
Router(config-router-af)# import path limit 3
Router(config-router-af)# end
```

Related Commands

Command	Description
import path selection	Specifies the BGP import path selection policy for a specific VRF instance.
show ip bgp vpnv4	Displays VPNv4 address information from the BGP table.

import path selection

To specify the Border Gateway Protocol (BGP) import path selection policy for a specific VPN routing and forwarding (VRF) instance, use the **import path selection** command in address family configuration mode. To remove the BGP import path selection policy for a VRF, use the **no** form of this command.

import path selection {**all** | **bestpath** [**strict**] | **multipaths** [**strict**]}

no import path selection {**all** | **bestpath** [**strict**] | **multipaths** [**strict**]}

Syntax Description

all	Imports all available paths from the exporting net that match any route targets (RTs) associated with the importing VRF instance. The number of paths imported per importing net must not exceed the import path limit set using the **import path limit** command.
bestpath	Imports the best available path that matches the RT of the VRF instance. If the best path in the exporting net does not match the RT of the VRF instance, a best available path that matches the RT of the VRF instance, is imported.
multipaths	Imports the bestpath and all paths marked as multipaths that match the RT of the VRF instance. If there are no bestpath or multipath matches, the best available path is selected. The number of paths imported per importing net must not exceed the import path limit set using the **import path limit** command.
strict	(Optional) Disables the fall back safety option of choosing the best available path for the **bestpath** and **multipath** keywords. If there are no paths appropriate to the configured option—bestpath or multipath—in the exporting net that match the RT of the VRF instance, then no paths are imported. This behavior matches the behavior of the software before the BGP Event-Based VPN Import feature was introduced.

Command Default

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

Command Modes

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

Command History

Release	Modification
15.0(1)M	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE 2.6	This command was integrated into Cisco IOS XE Release 12.6

Usage Guidelines

Use the **import path selection** command to set the import path policy for the BGP Event-Based VPN Import feature. Use the **import path limit** command to control memory utilization when importing paths by limiting the number of paths imported from an exporting net into each importing net.

The BGP Event-Based VPN Import feature introduces a modification to the existing BGP path import process. BGP Virtual Private Network (VPN) import provides importing functionality for BGP paths where BGP paths are imported from the BGP VPN table into a BGP virtual routing and forwarding (VRF) topology. In the existing path import process, when path updates occur, the import updates are processed during the next scan time which is a configurable interval of 5 to 15 seconds. The scan time adds a delay in the propagation of routes. The enhanced BGP path import is driven by events; when a BGP path changes, all of its imported copies are updated as soon as processing is available.

Using the BGP Event-Based VPN Import feature, convergence times are significantly reduced because provider edge (PE) routers can propagate VPN paths to customer edge (CE) routers without the scan time delay. Configuration changes such as adding imported route-targets to a VRF are not processed immediately, and are still handled during the 60-second periodic scanner pass.

Examples

The following example shows how to specify a BGP import path selection policy for a specific VRF instance. Two BGP neighbors are configured in BGP router configuration mode and are activated in VPNv4 address family configuration mode. In IPv4 VRF address family configuration mode, the import path selection is set to all, and the number of import paths is set to 3. In this example, up to three paths from an exporting net that match any of the route targets associated with the VRF of the importing net, can be imported.

```
Router(config)# router bgp 45000
Router(config-router)# neighbor 192.168.1.2 remote-as 40000
Router(config-router)# neighbor 192.168.3.2 remote-as 50000
Router(config-router)# address-family vpnv4
Router(config-router-af)# neighbor 192.168.1.2 activate
Router(config-router-af)# neighbor 192.168.3.2 activate
Router(config-router-af)# exit-address-family
Router(config-router)# address-family ipv4 vrf vrf-A
Router(config-router-af)# import path selection all
Router(config-router-af)# import path limit 3
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.
show ip bgp vpnv4	Displays VPNv4 address information from the BGP table.

import-map

To configure flexible policy handling by a BGP route server, use the **import-map** command in route server context address family configuration mode. To remove the route server's flexible policy handling, use the **no** form of this command.

import-map *route-map-name*

no import-map *route-map-name*

Syntax Description

route-map-name	Name of the route map that controls which routes will be added to the route server client virtual table.

Command Default

No import map exists and no flexible policy handling by a route server exists.

Command Modes

Route server context address family configuration (config-router-rsctx-af)

Command History

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

Usage Guidelines

Use this command if your BGP route server needs to support flexible policies.

In order to configure flexible policy handling, you must create a route server context, which includes an import map. The import map references a standard route map. You may match on nexthop, AS path, communities, and extended communities.

Note Do not confuse the **import-map** command with the **import map** command in VRF configuration submode, which configures an import route map for a VPN routing and forwarding (VRF) instance.

Examples

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
description (route server context)	Describes a route server context for a user-friendly way to see the purpose of the route server context.
route-map	Enables policy routing.
route-server-context	Creates a route-server context in order to provide flexible policy handling for a BGP route server.

inherit peer-policy

To configure a peer policy template to inherit the configuration from another peer policy template, use the **inherit peer-policy** command in policy-template configuration mode. To remove an inherit statement from a peer policy template, use the **no** form of this command.

inherit peer-policy *policy-template sequence-number*

no inherit peer-policy *policy-template sequence-number*

Syntax Description

policy -template	Name of the peer policy template to be inherited.
sequence-number	Sequence number that sets the order in which the peer policy template is evaluated. Like a route-map sequence number, the lowest sequence number is evaluated first.

Defaults

No inherit statements are configured.

Command Modes

Policy-template configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
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 **inherit peer-policy** command is used to configure a peer policy template to inherit the configuration of another peer policy template. Peer policy templates support inheritance and a peer can directly and indirectly inherit up to seven peer policy templates. Inherited peer policy templates are configured with sequence numbers like route maps. An inherited peer policy template, like a route map, is evaluated starting with the inherit statement with the lowest sequence number. However, peer policy templates do not fall through. Every sequence is evaluated. If a BGP policy command is reapplied with a different value, it will overwrite any previous value from a lower sequence number.

Note A Border Gateway Protocol (BGP) routing process cannot be configured to be a member of a peer group and to use peer templates for group configurations. You must use one method or the other. We recommend peer templates because they provide improved performance and scalability.

Examples

In the following example, a peer policy template named CUSTOMER-A is created. This peer policy template is configured to inherit the configuration from the peer policy templates named PRIMARY-IN and GLOBAL.

```
Router(config-router)# template peer-policy CUSTOMER-A
Router(config-router-ptmp)# route-map SET-COMMUNITY in
Router(config-router-ptmp)# filter-list 20 in
Router(config-router-ptmp)# inherit peer-policy PRIMARY-IN 20
Router(config-router-ptmp)# inherit peer-policy GLOBAL 10
Router(config-router-ptmp)# exit-peer-policy
Router(config-router)#
```

Related Commands

Command	Description
exit peer-policy	Exits policy-template configuration mode and enters router configuration mode.
neighbor inherit peer-policy	Configures a router to send a peer policy template to a neighbor so that the neighbor can inherit the configuration.
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.

inherit peer-session

To configure a peer session template to inherit the configuration from another peer session template, use the **inherit peer-session** command in session-template configuration mode. To remove an inherit statement from a peer session template, use the **no** form of this command.

inherit peer-session *template-name*

no inherit peer-session *template-name*

Syntax Description

template-name	Name of the peer session template to inherit.

Defaults

No inherit statements are configured.

Command Modes

Session-template 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

The **inherit peer-session** command is used to configure a peer session template to inherit the configuration of another peer session template. A peer can be configured with only one peer session template at a time, and that peer session template can contain only one indirectly inherited peer session template. However, each indirectly inherited session template can also contain an indirectly inherited template. So, a peer can directly inherit only one peer session template and indirectly inherit up to seven additional indirectly inherited peer session templates, allowing you to apply up to a maximum of eight inherited peer session configurations.

Note If you attempt to configure more than one inherit statement with a single peer session template, an error message will be displayed.

Indirectly inherited peer session templates are evaluated first, and the directly applied (locally configured) peer session template is evaluated last. If a general session command is reapplied with a different value, the subsequent value will have priority and overwrite the previous value that was configured in the indirectly inherited template. In other words, an overlapping statement from a local configuration will override the statement from the inherited configuration.

Examples

In the following example, a peer session template named CORE1 is created. This example inherits the configuration of the peer session template named INTERNAL-BGP.

```
Router(config-router)# template peer-session CORE1
Router(config-router-stmp)# description CORE-123
Router(config-router-stmp)# update-source loopback 1
Router(config-router-stmp)# inherit peer-session INTERNAL-BGP
Router(config-router-stmp)# exit-peer-session
Router(config-router)#
```

Related Commands

Command	Description
exit peer-session	Exits session-template configuration mode and enters router configuration mode.
neighbor inherit peer-session	Configures a router to send a peer session template to a neighbor so that the neighbor can inherit the configuration.
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.

ip as-path access-list

To configure an autonomous system path filter using a regular expression, use the **ip as-path access-list** command in global configuration mode. To delete the autonomous system path filter and remove it from the running configuration file, use the **no** form of this command.

ip as-path access-list *acl-number* {**permit** | **deny**} *regexp*

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

Syntax Description

acl-number	Number from 1 to 500 that specifies the AS-path access-list number.
permit	Permits advertisement based on matching conditions.
deny	Denies advertisement based on matching conditions.
regexp	Regular expression that defines the AS-path filter. The autonomous system number is expressed 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. **Note** See the "Regular Expressions" appendix in the *Cisco IOS Terminal Services Configuration Guide* for information about configuring regular expressions.

Command Default

No autonomous system path filter is created.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.0(22)S	This command was modified. The range of values that can be entered for the *acl-number* argument was increased from 199 to 500 in Cisco IOS Release 12.0(22)S.
12.2(15)T	This command was modified. The range values that can be entered for the *acl-number* argument was increased 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.

Release	Modification
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX.
12.0(32)S12	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(24)T	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.3	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SXI1	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
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

Use the **ip as-path access-list** command to configure an autonomous system path filter. You can apply autonomous system path filters to both inbound and outbound BGP paths. Each filter is defined by the regular expression. If the regular expression matches the representation of the autonomous system path of the route as an ASCII string, then the **permit** or **deny** condition applies. The autonomous system path should not contain the local autonomous system number.

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. When the asdot format is enabled as the default, any regular expressions to match 4-byte autonomous system numbers must be written using the asdot format, or the regular expression match will fail.

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.

Examples

In the following example, an autonomous system path access list (number 500) is defined to configure the router to not advertise any path through or from autonomous system 65535 to the 10.20.2.2 neighbor:

```
ip as-path access-list 500 deny _65535_
ip as-path access-list 500 deny ^65535$
router bgp 50000
```

```
 neighbor 192.168.1.1 remote-as 65535
 neighbor 10.20.2.2 remote-as 40000
 neighbor 10.20.2.2 filter-list 500 out
 end
```

In the following example, the router is configured to deny all updates with private autonomous system paths:

```
ip as-path access-list 1 deny (_64[6-9][0-9][0-9]_|_65[0-9][0-9][0-9]_)
ip as-path access-list 1 permit .*
```

The following example available 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, shows BGP path filtering by neighbor using 4-byte autonomous system numbers in asplain format. Only the routes that pass autonomous system path access list 2 will be sent to 192.168.3.2.

```
ip as-path access-list 2 permit ^65536$
router bgp 65538
 neighbor 192.168.3.2 remote-as 65550
 address-family ipv4 unicast
  neighbor 192.168.3.2 filter-list 2 in
  end
```

The following example shows BGP path filtering by neighbor using 4-byte autonomous system numbers in asdot format. The dot notation is the only format for 4-byte autonomous system numbers in Cisco IOS Release 12.0(32)S12, 12.4(24)T, or Cisco IOS XE Release 2.3. This example can also be configured 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 later releases. after the **bgp asnotation dot** command has been entered to allow matching of 4-byte autonomous system numbers in regular expressions in asdot notation. The dot in the asdot notation is a special character for regular expressions and a backslash must precede it, as shown in the example. Only the routes that pass autonomous system path access list 2 will be sent to 192.168.3.2.

```
ip as-path access-list 2 permit ^1\.0$
router bgp 1.2
 neighbor 192.168.3.2 remote-as 1.14
 address-family ipv4 unicast
  neighbor 192.168.3.2 filter-list 2 in
  end
```

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 distribute-list	Distributes BGP neighbor information as specified in an access list.
neighbor filter-list	Applies a filter list to the specified neighbor.
neighbor prefix-list	Applies a prefix list to the specified neighbor.
router bgp	Configures the BGP routing process.

ip bgp fast-external-fallover

To configure per-interface fast external fallover, use the **ip bgp fast-external-fallover** command in interface configuration mode. To remove a per-interface fast external fallover configuration, use the **no** form of this command.

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

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

Syntax Description

permit	(Optional) Allows per-interface fast external fallover.
deny	(Optional) Prevents per-interface fast external fallover.

Defaults

Global fast external fallover is enabled by default in Cisco IOS software.

Command Modes

Interface configuration

Command History

Release	Modification
12.0ST	This command was introduced.
12.1	This command was integrated into Cisco IOS Release 12.1.
12.2(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 **ip bgp fast-external-fallover** command is used to configure per-interface fast external fallover, overriding the global configuration. Entering the **permit** keyword enables fast external fallover. Entering the **deny** keyword disables fast external fallover. Entering the **no** form of this command, returns the router to the global configuration.

Examples

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

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

Related Commands

Command	Description
bgp fast-external-fallover	Configures global BGP fast external fall over.

ip bgp-community new-format

To configure BGP to display communities in the format AA:NN (autonomous system:community number/4-byte number), use the **ip bgp-community new-format** command in global configuration mode. To configure BGP to display communities as a 32-bit number, use the **no** form of this command.

ip bgp-community new-format

no ip bgp-community new-format

Syntax Description

This command has no argument or keywords.

Defaults

BGP communities (also when entered in the AA:NN format) are displayed as a 32-bit numbers if this command is not enabled or if the **no** form is entered.

Command Modes

Global 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 **ip bgp-community new-format** command is used to configure the local router to display BGP communities in the AA:NN format to conform with RFC-1997. This command only affects the format in which BGP communities are displayed; it does not affect the community or community exchange. However, expanded IP community lists that match locally configured regular expressions may need to be updated to match on the AA:NN format instead of the 32-bit number.

RFC 1997, *BGP Communities Attribute*, specifies that a BGP community is made up of two parts that are each 2 bytes long. The first part is the autonomous system number and the second part is a 2-byte number defined by the network operator.

Examples

In the following example, a router that uses the 32-bit number community format is upgraded to use the AA:NN format:

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

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

```
Router# show ip bgp 10.0.0.0

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

Related Commands

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

ip community-list

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

Standard Community Lists

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

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

Expanded Community Lists

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

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

Syntax Description

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

expanded *list-name*	Configures a named expanded community list.
regexp	Configures a regular expression that is used to specify a pattern to match against an input string. **Note** Regular expressions can be used only with expanded community lists

Command Default

BGP community exchange is not enabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.3	This command was introduced.
12.0	Support for the **local-as** community was introduced.
12.0(10)S	Named community list support was added.
12.0(16)ST	Named community list support was introduced.
12.1(9)E	Named community list support was integrated into Cisco IOS Release 12.1(9)E.
12.2(8)T	Named community list support was integrated into Cisco IOS Release 12.2(8)T.
12.0(22)S	The maximum number of expanded community list numbers was increased from 199 to 500.
12.2(14)S	The maximum number of expanded community list numbers was increased from 199 to 500 and named community list support were integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	The maximum number of expanded community list numbers was increased from 199 to 500.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	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 **ip community-list** command is used to configure BGP community filtering. BGP community values are configured as a 32-bit number (old format) or as a 4-byte number (new format). The new community format is enabled when the **ip bgp-community new-format** command is entered in global configuration mode. The new community format consists of a 4-byte value. The first two bytes represent the autonomous system number, and the trailing two bytes represent a user-defined network number. Named and numbered community lists are supported. BGP community attribute exchange between BGP peers is enabled when the **neighbor send-community** command is configured for the specified neighbor. The BGP community attribute is defined in RFC 1997 and RFC 1998.

BGP community exchange is not enabled by default. It is enabled on a per-neighbor basis with the **neighbor send-community** command. The Internet community is applied to all routes or prefixes by default, until any other community value is configured with this command or the **set community** command.

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

Standard Community Lists

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

Expanded Community Lists

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

Community List Processing

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

Examples

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

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

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

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

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

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

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

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

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

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

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

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

Related Commands

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

ip extcommunity-list

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

Global Configuration Mode CLI

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

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

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

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

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

Expanded IP Extended Community-List Configuration Mode CLI

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

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

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

Standard IP Extended Community-List Configuration Mode CLI

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

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

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

Syntax Description

expanded-list	An expanded list number from 100 to 500 that identifies one or more permit or deny groups of extended communities.
standard-list	A standard list number from 1 to 99 that identifies one or more permit or deny groups of extended communities.
expanded *list-name*	Creates an expanded named extended community list and enters IP Extended community-list configuration mode.

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

Command Default

Extended community exchange is not enabled by default.

Command Modes

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

Command History

Release	Modification
12.1	This command was introduced.
12.0(22)S	The maximum number of expanded community list numbers was increased from 199 to 500.
12.2(15)T	The maximum number of expanded community list numbers was increased from 199 to 500.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2(25)S	Support for the following was added in Cisco IOS Release 12.2(25)S: • Extended community-list sequencing • IP Extended community configuration mode • Named extended community lists
12.3(11)T	Support for the following was added in Cisco IOS Release 12.3(11)T: • Extended community-list sequencing • IP Extended community configuration mode • Named extended community lists
12.2(27)SBC	This command was integrated into the Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(14)SX	This command was integrated into the Cisco IOS Release 12.2(14)SX.
12.0(32)S12	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(24)T	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
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 **ip extcommunity-list** command is used to configure named or numbered extended community lists. Extended community attributes are used to filter routes for VPN routing and forwarding instances (VRFs) and Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs). All of the standard rules of access lists apply to the configuration of extended community lists. The route target (RT) and site of origin (SOO) extended community attributes are supported by the standard range of extended community lists. Extended community list entries start with the number 10 and increment by ten for each subsequent entry when no sequence number is specified, when default behavior is configured, and when an extended community list is resequenced without specifying the first entry number or the increment range for subsequent entries. Regular expressions are supported in expanded extended community lists. For information about configuring regular expressions, see the “Regular Expressions” appendix of the *Cisco IOS Terminal Services Configuration Guide*.

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

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

Route Target Extended Community Attribute

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

Site of Origin Extended Community Attribute

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

IP Extended Community-List Configuration Mode

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

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

Extended Community List Processing

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

Examples

Standard Extended Community-List Configuration Example

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

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

Expanded Extended Community-List Configuration Example

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

```
Router(config)# ip extcommunity-list 500 deny _65412_
Router(config)# router bgp 50000
Router(config-router)# address-family vpnv4
Router(config-router-af)# neighbor 172.16.1.1 remote-as 65412
Router(config-router-af)# neighbor 172.16.1.1 neighbor send-community extended
Router(config-router-af)# neighbor 192.168.1.2 remote-as 65534
Router(config-router-af)# neighbor 192.168.1.2 neighbor send-community extended
Router(config-router-af)# end
```

Named Extended Community-List Configuration Example

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

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

IP Extended Community-List Configuration Mode Example

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

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

Extended Community-List Resequencing Example

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

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

4-Byte Autonomous System Support for Extended Community-List Examples

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

```
Router(config)# ip extcommunity-list expanded DENY65550
```

```
Router(config-extcomm-list)# 10 deny _65550_
Router(config-extcomm-list)# 20 deny ^65550 .*
Router(config-extcomm-list)# resequence 50 100
Router(config-extcomm-list)# exit
Router(config)# router bgp 65538
Router(config-router)# network 172.17.1.0 mask 255.255.255.0
Router(config-router)# neighbor 192.168.3.2 remote-as 65550
Router(config-router)# neighbor 192.168.1.2 remote-as 65536
Router(config-router)# neighbor 192.168.3.2 activate
Router(config-router)# neighbor 192.168.1.2 activate
Router(config-router)# end
Router# show ip extcommunity-list DENY65550
```

In Cisco IOS Release 12.0(32)SY8, 12.0(32)S12, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, 12.4(24)T, and Cisco IOS XE Release 2.3, or a later releases, extended BGP communities support 4-byte autonomous system numbers in the regular expressions in asdot format. In this task, the router is configured with an extended named community list to specify that the BGP peer at 192.168.1.2 is not sent advertisements about any path through or from the 4-byte autonomous system 1.14. The IP extended community-list configuration mode is used, and the ability to resequence entries is shown.

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

Related Commands

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

ip policy-list

To create a Border Gateway Protocol (BGP) policy list, use the **ip policy-list** command in policy-map configuration mode. To remove a policy list, use the **no** form of this command.

ip policy-list *policy-list-name* {**permit** | **deny**}

no ip policy-list *policy-list-name*

Syntax Description

policy-list-name	Name of the configured policy list.
permit	Permits access for matching conditions.
deny	Denies access to matching conditions.

Defaults

This command is not enabled by default.

Command Modes

Global configuration mode

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 configured within a route map are evaluated with AND semantics or OR semantics. A policy list can also coexist with any other preexisting match and set statements that are configured within the same route map but outside of the policy list. When multiple policy lists perform matching within a route map entry, all policy lists match on the incoming attribute only.

Examples

In the following example, a policy list is configured that permits all network prefixes that match AS 1 and metric 10:

```
Router(config)# ip policy-list POLICY-LIST-NAME-1 permit
Router(config-policy-list)# match as-path 1
Router(config-policy-list)# match metric 10
Router(config-policy-list)# end
```

In the following example, a policy list is configured that permits traffic that matches community 20 and metric 10:

```
Router(config)# ip policy-list POLICY-LIST-NAME-2 permit
Router(config-policy-list)# match community 20
Router(config-policy-list)# match metric 10
Router(config-policy-list)# end
```

In the following example, a policy list is configured that denies traffic that matches community 20 and metric 10:

```
Router(config)# ip policy-list POLICY-LIST-NAME-3 deny
Router(config-policy-list)# match community 20
Router(config-policy-list)# match metric 10
Router(config-policy-list)# end
```

Related Commands

Command	Description
match as-path	References a policy list within a route map for evaluation and processing.
show ip policy-list	Displays configured policy lists.
show route-map	Displays configured route maps and information about referenced policy maps.

ip prefix-list

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

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

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

Syntax Description

list-name	Configures a name to identify the prefix list. Do not use the word "detail" or "summary" as a list name because they are keywords in the **show ip prefix-list** command.
seq	(Optional) Applies a sequence number to a prefix-list entry.
number	(Optional) Integer from 1 to 4294967294. If a sequence number is not entered when configuring this command, default sequence numbering is applied to the prefix list. The number 5 is applied to the first prefix entry, and subsequent unnumbered entries are incremented by 5.
deny	Denies access for a matching condition.
permit	Permits access for a matching condition.
network/length	Configures the network address and the length of the network mask in bits. The network number can be any valid IP address or prefix. The bit mask can be a number from 1 to 32.
ge	(Optional) Specifies the lesser value of a range (the "from" portion of the range description) by applying the *ge-length* argument to the range specified. **Note** The **ge** keyword represents the greater than or equal to operator.
ge-length	(Optional) Represents the minimum prefix length to be matched.
le	(Optional) Specifies the greater value of a range (the "to" portion of the range description) by applying the *le-length* argument to the range specified. **Note** The **le** keyword represents the less than or equal to operator.
le-length	(Optional) Represents the maximum prefix length to be matched.
description	(Optional) Configures a descriptive name for the prefix list.
description	(Optional) Descriptive name of the prefix list, from 1 to 80 characters in length.
sequence-number	(Optional) Enables or disables the use of sequence numbers for prefix lists.

Command Default

No prefix lists or prefix-list entries are created.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

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

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

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

The following formula shows this behavior:

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

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

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

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

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

Examples

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

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

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

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

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

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

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

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

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

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

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

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

Related Commands

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

ip prefix-list description

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

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

no ip prefix-list *list-name* **description**

Syntax Description

list-name	Identifies the prefix-list that is being described.
text	Adds a text description. Up to 80 characters can be entered.

Defaults

No default behavior or values

Command Modes

Global 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

Use the **ip prefix-list description** command to add a helpful description to an IP prefix list, which you can see in the configuration file and in the **show ip prefix-list** output to remind you what the prefix list is for. The description can be up to 80 characters in length.

Examples

In the following example, a description is added to the prefix list named RED, which indicates that the prefix list is to permit routes from network A:

```
Router(config)# ip prefix-list RED description Permit routes from network A
```

Related Commands

Command	Description
clear ip prefix-list	Resets the prefix list entry counters.
ip prefix-list	Creates an entry in a prefix list.
ip prefix-list sequence	Enables or disables default prefix-list sequencing.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.

neighbor prefix-list	Filters routes from the specified neighbor using a prefix list.
show ip prefix-list	Displays information about a prefix list or prefix list entries.

ip prefix-list sequence-number

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

ip prefix-list sequence-number

no ip prefix-list sequence-number

Syntax Description

This command has no arguments or keywords.

Defaults

Default sequence numbers are generated when an IP prefix list is configured.

Command Modes

Global 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.

Examples

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

```
Router(config)# no ip prefix-list sequence-number
```

Related Commands

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

ip verify unicast vrf

To enable Unicast Reverse Path Forwarding (Unicast RPF) verification for a specified VRF, use the **ip verify unicast vrf** command in interface configuration mode. To disable the Unicast RPF check for a VRF, use the **no** form of this command.

ip verify unicast vrf *vrf-name* {**deny** | **permit**}

no ip verify unicast vrf *vrf-name* {**deny** | **permit**}

Syntax Description

vrf-name	Virtual Private Network (VPN) routing and forwarding (VRF) instance name.
deny	Specifies that traffic associated with the specified VRF is dropped after it passes the Unicast RPF verification.
permit	Specifies that traffic associated with the specified VRF is forwarded after it passes the Unicast RPF verification.

Command Default

Unicast RPF verification is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(29)S	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(28)SB	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.

Usage Guidelines

Unicast RPF is configured to verify that the source address is in the Forwarding Information Base (FIB). The **ip verify unicast vrf** command is configured in interface configuration mode and is enabled for each VRF. This command has **permit** and **deny** keywords that are used to determine if traffic is forwarded or dropped after Unicast RPF verification.

Examples

The following example configures Unicast RPF verification for VRF1 and VRF2. VRF1 traffic is forwarded. VRF2 traffic is dropped.

```
Router(config)# interface Ethernet 0
Router(config-if)# ip verify unicast vrf vrf1 permit
Router(config-if)# ip verify unicast vrf vrf2 deny
Router(config-if)# end
```

Related Commands

Command	Description
import ipv4	Configures an import map to import IPv4 prefixes from the global routing table to a VRF table.
ip vrf	Configures a VRF routing table.
rd	Creates routing and forwarding tables for a VRF.
show ip bgp	Displays entries in the BGP routing table.
show ip bgp vpnv4	Displays VPN address information from the BGP table.
show ip vrf	Displays the set of defined VRFs and associated interfaces.