BGP Commands: A through B

activate (bmp)

To initiate a connection between BGP monitoring protocol (BMP) server and BGP neighbors, use the **activate** command in BMP server configuration mode. To stop the connection, use the **no** form of the command.

activate

no activate

Command Default

No connectivity is established between BMP servers and BGP BMP neighbors.

Command Modes

BMP server configuration (config-router-bmpsrvr)

Command History

Release	Modification
15.4(1)S	This command was introduced.
Cisco IOS XE Release 3.11S	This command was integrated into Cisco IOS XE Release 3.11S.

Usage Guidelines

Use the **bmp server** command to enter BMP server configuration mode and configure a specific BMP server. To configure BGP BMP neighbors to which the BMP servers establish a connection, use the **neighbor bmp-activate** command in router configuration mode. Use the **show ip bgp bmp** command to verify whether the connection is established or not.

Example

The following example show how to enter BMP server configuration mode and initiate connection between a specific BMP server with the BGP BMP neighbors. In this example, connection is initiated to BMP server 1 and BMP server 2:

```
Device> enable
Device# configure terminal
Device(config)# router bgp 65000
Device(config-router)# bmp server 1
Device(config-router-bmpsrvr)# activate
Device(config-router-bmpsrvr)# exit-bmp-server-mode
Device(config-router)# bmp server 2
Device(config-router-bmpsrvr)# activate
Device(config-router-bmpsrvr)# end
```

The following is sample output from the **show ip bgp bmp server** command for BMP server number 1 and 2. The output displays “activated” which indicates that the connection between the two servers has been established with the BGP BM neighbors:

```
Device# show ip bgp bmp server 1

Print detailed info for 1 server number 1.

bmp server 1
address: 10.1.1.1    port 8000
description SERVER1
up time 00:06:22
```

```
session-startup route-refresh
initial-delay 20
failure-retry-delay 40
flapping-delay 120
activated

Device# show ip bgp bmp server 2

Print detailed info for 1 server number 2.

bmp server 2
address: 20.1.1.1    port 9000
description SERVER2
up time 00:06:23
session-startup route-refresh
initial-delay 20
failure-retry-delay 40
flapping-delay 120
activated
```

Related Commands

Command	Description
bmp server	Enters BMP server configuration mode to configure specific BMP servers.
neighbor bmp-activate	Activates BMP monitoring for BGP neighbors.
show ip bgp bmp	Displays information about BMP servers and neighbors.

additional-paths

To use a policy template to configure BGP to send or receive additional paths, use the **additional-paths** command in policy template configuration mode. To remove the policy from the current template, use the **no** form of this command.

additional-paths {**send** [**receive**] | **receive** | **disable**}
no additional-paths

Syntax Description

send	(Optional) Enables BGP to send additional paths.
receive	(Optional) Enables BGP to receive additional paths.
disable	(Optional) Overrides any address family configuration that enable the sending or receiving of additional paths. The **disable** keyword cannot be used with the **send** or **receive** keyword.

Command Default

No additional paths are sent or received using a policy template.

Command Modes

Policy template configuration (config-router-ptmp)

Command History

Release	Modification
15.2(4)S	This command was introduced.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.
15.3(1)T	This command was integrated into Cisco IOS Release 15.3(1)T.

Usage Guidelines

The **additional-paths** command is part of a template; the syntax differs from the global **bgp additional-paths** command. The ability to send and receive additional paths is negotiated between two BGP neighbors during session establishment.

Keep in mind that in order to advertise this path, you also need to:

- Select the path (other than best-path)
- Advertise that advertise-set (other than best-path) by using the **advertise additional-paths** command.

The **no additional-paths** command removes the policy from the current template. A peer applying this policy might still be subject to the address-family-wide **bgp additional-paths** command.

Use the **show ip bgp neighbors** command to display whether neighbors are capable of sending or receiving additional paths. Use the **show ip bgp** command with a network address to display the path selections and path IDs.

Examples

In the following example, the template is configured to allow additional path sending and receiving.

```
router bgp 45000
address-family ipv4 unicast
 bgp additional-paths send receive
 bgp additional-paths select group-best best 3
```

```
template peer-policy rr-client-pt1
 additional-paths send receive
 advertise additional-paths best 3
 exit
address-family ipv4 unicast
 neighbor 192.168.1.1 remote-as 45000
 neighbor 192.168.1.1 inherit peer-policy rr-client-pt1
 end
```

Related Commands

Command	Description
advertise additional-paths	Advertises BGP additional paths based on selection.
bgp additional-paths	Configures BGP to send or receive additional paths for all neighbors in the address family.
neighbor additional-paths	Configures the local router with the ability to send and receive additional path information for a neighbor or peer group.
neighbor inherit peer-policy	Sends a peer policy template to a neighbor so that the neighbor can inherit the configuration.
show ip bgp	Displays information about BGP networks, including path selections and path IDs.
show ip bgp neighbors	Displays information about the TCP and BGP connections of neighbors.
template peer-policy	Creates a peer policy template and enters policy template configuration mode.

address (bmp)

To configure IP address and port number to a specific BGP Monitoring Protocol (BMP) server, use the **address** command in BMP server configuration mode. To remove the IP address and the port number, use the **no** form of the command.

address {*ipv4-addr ipv6-addr*} **port-number** *port-number*

no address {*ipv4-addr ipv6-addr*} **port-number** *port-number*

Syntax Description

ipv4-addr	Configures an IPv4 address on the BMP server.
ipv6-addr	Configures an IPv6 address on the BMP server.
port-number *port-number*	Configures the listening port of the BMP server. The port-number of the listening BMP server ranges from 1 to 65535.

Command Default

IP address and port number is not configured for the BMP server.

Command Modes

BMP server configuration (config-router-bmpsrvr)

Command History

Release	Modification
15.4(1)S	This command was introduced.
Cisco IOS XE Release 3.11S	This command was integrated into Cisco IOS XE Release 3.11S.

Usage Guidelines

Use the **bmp server** command to enter BMP server configuration mode and configure a specific BMP server. To configure BGP BMP neighbors to which the BMP servers establish a connection, use the **neighbor bmp-activate** command in router configuration mode. Use the **show ip bgp bmp** command to verify that IP address and port number have been configured.

Example

The following example show how to enter BMP server configuration mode and assign IP address and port number for BMP server 1 and 2:

```
Device> enable
Device# configure terminal
Device(config)# router bgp 65000
Device(config-router)# bmp server 1
Device(config-router-bmpsrvr)# activate
Device(config-router-bmpsrvr)# address 10.1.1.1 port-number 8000
Device(config-router-bmpsrvr)# exit-bmp-server-mode
Device(config-router)# bmp server 2
Device(config-router-bmpsrvr)# activate
Device(config-router-bmpsrvr)# address 20.1.1.1 port-number 9000
Device(config-router-bmpsrvr)# end
```

The following is sample output from the **show ip bgp bmp server** command for BMP server number 1 and 2. The “address” and the “port” field in the output display the IP address and the port number of the listening BMP servers 1 and 2:

```
Device# show ip bgp bmp server 1

Print detailed info for 1 server number 1.

bmp server 1
address: 10.1.1.1    port 8000
description SERVER1
up time 00:06:22
session-startup route-refresh
initial-delay 20
failure-retry-delay 40
flapping-delay 120
activated

Device# show ip bgp bmp server 2

Print detailed info for 1 server number 2.

bmp server 2
address: 20.1.1.1    port 9000
description SERVER2
up time 00:06:23
session-startup route-refresh
initial-delay 20
failure-retry-delay 40
flapping-delay 120
activated
```

Related Commands

Command	Description
bmp server	Enters BMP server configuration mode to configure specific BMP servers.
neighbor bmp-activate	Activates BMP monitoring for BGP neighbors.
show ip bgp bmp	Displays information about BMP servers and neighbors.

address-family ipv4 (BGP)

To enter address family or router scope address family configuration mode to configure a routing session using standard IP Version 4 (IPv4) address prefixes, use the **address-family ipv4** command in router configuration or router scope configuration mode. To exit address family configuration mode and remove the IPv4 address family configuration from the running configuration, use the **no** form of this command.

Syntax Available Under Router Configuration Mode
address-family ipv4 [**mdt** | **tunnel** | {**multicast** | **unicast**} [**vrf** *vrf-name*] | **vrf** *vrf-name*]
no address-family ipv4 [**mdt** | **tunnel** | {**multicast** | **unicast**} [**vrf** *vrf-name*] | **vrf** *vrf-name*]

Syntax Available Under Router Scope Configuration Mode
address-family ipv4 [**mdt** | **multicast** | **unicast**]
no address-family ipv4 [**mdt** | **multicast** | **unicast**]

Syntax Description

mdt	(Optional) Specifies an IPv4 multicast distribution tree (MDT) address family session.
tunnel	(Optional) Specifies an IPv4 routing session for multipoint tunneling.
multicast	(Optional) Specifies IPv4 multicast address prefixes.
unicast	(Optional) Specifies IPv4 unicast address prefixes. This is the default.
vrf *vrf-name*	(Optional) Specifies the name of the VPN routing and forwarding (VRF) instance to associate with subsequent IPv4 address family configuration mode commands.

Command Default

IPv4 address prefixes are not enabled.

Command Modes

Router configuration (config-router)

Router scope configuration (config-router-scope)

Command History

Release	Modification
12.0(5)T	This command was introduced. This command replaced the **match nlri** and **set nlri** commands.
12.0(28)S	This command was modified. The **tunnel** keyword was added.
12.0(29)S	This command was modified. The **mdt** keyword was added.
12.0(30)S	This command was modified. Support for the Cisco 12000 series Internet router 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(33)SRB	This command was modified. Support for router scope configuration mode was added. The **tunnel** keyword was deprecated.

Release	Modification
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Aggregation Services Routers.
12.4(20)T	This command was modified. The **mdt** keyword was added. The **tunnel** keyword was deprecated.
Cisco IOS XE Release 3.6S	This command was modified. VRF-based multicast support was added.
15.2(4)S	This command was implemented on the Cisco 7200 series router.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

The **address-family ipv4** command replaces the **match nlri** and **set nlri** commands. The **address-family ipv4** command places the device in address family configuration mode (prompt: config-router-af), from which you can configure routing sessions that use standard IPv4 address prefixes. To leave address family configuration mode and return to router configuration mode, type **exit**.

Note Routing information for address family IPv4 is advertised by default for each Border Gateway Protocol (BGP) routing session configured with the **neighbor remote-as** command unless you enter the **no bgp default ipv4-unicast** command before configuring the **neighbor remote-as** command.

The **tunnel** keyword is used to enable the tunnel subaddress family identifier (SAFI) under the IPv4 address family identifier. This SAFI is used to advertise the tunnel endpoints and the SAFI-specific attributes (which contain the tunnel type and tunnel capabilities). Redistribution of tunnel endpoints into the BGP IPv4 tunnel SAFI table occurs automatically when the tunnel address family is configured. However, peers need to be activated under the tunnel address family before the sessions can exchange tunnel information.

The **mdt** keyword is used to enable the MDT SAFI under the IPv4 address family identifier. This SAFI is used to advertise tunnel endpoints for inter-AS multicast VPN peering sessions.

If you specify the **address-family ipv4 multicast** command, you will then specify the **network** *network-number* [**mask** *network-mask*] command. The **network** command advertises (injects) the specified network number and mask into the multicast BGP database. This route must exist in the forwarding table installed by an Interior Gateway Protocol (IGP) (that is, by EIGRP, OSPF, RIP, IGRP, static, or IS-IS), but not BGP.

In Cisco IOS Release 12.2(33)SRB and later releases, the ability to use address family configuration under the router scope configuration mode was introduced. The scope hierarchy can be defined for BGP routing sessions and is required to support Multitopology Routing (MTR). To enter the router scope configuration mode, use the **scope** command, which can apply globally or for a specific VRF. When using the scope for a specific VRF, only the **unicast** keyword is available.

Examples

The following example places the device in address family configuration mode for the IPv4 address family:

```
Device(config)# router bgp 50000
Device(config-router)# address-family ipv4
Device(config-router-af)#
```

The following example places the device in address family configuration mode and specifies only multicast address prefixes for the IPv4 address family:

```
Device(config)# router bgp 50000
Device(config-router)# address-family ipv4 multicast
Device(config-router-af)#
```

The following example places the device in address family configuration mode and specifies unicast address prefixes for the IPv4 address family:

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

The following example places the device in address family configuration mode and specifies **cisco** as the name of the VRF instance to associate with subsequent IPv4 address family configuration mode commands:

```
Device(config)# router bgp 50000
Device(config-router)# address-family ipv4 vrf cisco
Device(config-router-af)#
```

Note Use this form of the command, which specifies a VRF, only to configure routing exchanges between provider edge (PE) and customer edge (CE) devices.

The following example places the device in tunnel address family configuration mode:

```
Device(config)# router bgp 100
Device(config-router)# address-family ipv4 tunnel
Device(config-router-af)#
```

The following example shows how to configure a device to support an IPv4 MDT address-family session:

```
Device(config)# router bgp 45000
Device(config-router)# address-family ipv4 mdt
Device(config-router-af)#
```

The following example shows how to configure the IPv4 address family under router scope configuration mode. In this example, the scope hierarchy is enabled globally. The device enters router scope address family configuration mode, and only multicast address prefixes for the IPv4 address family are specified:

```
Device(config)# router bgp 50000
Device(config-router)# scope global
Device(config-router-scope)# address-family ipv4 multicast
Device(config-router-scope-af)#
```

Related Commands

Command	Description
address-family ipv6	Places the device in address family configuration mode for configuring routing sessions, such as BGP, that use standard IPv6 address prefixes.
address-family vpn4	Places the device in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPN Version 4 address prefixes.
bgp default ipv4-unicast	Enables the IPv4 unicast address family on all neighbors.
neighbor activate	Enables the exchange of information with a BGP neighboring device.
neighbor remote-as	Adds an entry to the BGP or multiprotocol BGP neighbor table.
scope	Defines the scope for a BGP routing session and enters router scope configuration mode.

address-family l2vpn

To enter address family configuration mode to configure a routing session using Layer 2 Virtual Private Network (L2VPN) endpoint provisioning address information, use the **address-family l2vpn** command in router configuration mode. To remove the L2VPN address family configuration from the running configuration, use the **no** form of this command.

address-family l2vpn [**evpn | vpls**]
no address-family l2vpn [**evpn | vpls**]

Syntax Description

evpn	(Optional) Specifies L2VPN Ethernet Virtual Private Network (EVPN) endpoint provisioning address information.
vpls	(Optional) Specifies L2VPN Virtual Private LAN Service (VPLS) endpoint provisioning address information.

Command Default

No L2VPN endpoint provisioning support is enabled.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.
15.1(1)S	This command was integrated into Cisco IOS Release 15.1(1)S.
Cisco IOS XE Release 3.11S	This command was modified. The **evpn** keyword was added.

Usage Guidelines

The **address-family l2vpn** command places the router in address family configuration mode (prompt: config-router-af), from which you can configure routing sessions that support L2VPN endpoint provisioning.

BGP support for the L2VPN address family introduces a BGP-based autodiscovery mechanism to distribute L2VPN endpoint provisioning information. BGP uses a separate L2VPN routing information base (RIB) to store endpoint provisioning information, which is updated each time any Layer 2 (L2) virtual forwarding instance (VFI) is configured. Prefix and path information is stored in the L2VPN database, allowing BGP to make best-path decisions. When BGP distributes the endpoint provisioning information in an update message to all its BGP neighbors, the endpoint information is used to set up a pseudowire mesh to support L2VPN-based services.

The BGP autodiscovery mechanism facilitates the setting up of L2VPN services, which are an integral part of the Cisco IOS Virtual Private LAN Service (VPLS) feature. VPLS enables flexibility in deploying services by connecting geographically dispersed sites as a large LAN over high-speed Ethernet in a robust and scalable IP MPLS network.

The multiprotocol capability for address family L2VPN EVPN is advertised when the Address Family Identifier (AFI) is enabled under the internal BGP (iBGP) and external BGP (eBGP) neighbors for both IPv4 and IPv6 neighbors.

Note Routing information for address family IPv4 is advertised by default for each BGP routing session configured with the **neighbor remote-as** command unless you configure the **no bgp default ipv4-unicast** command before configuring the **neighbor remote-as** command.

Examples

In this example, two provider edge (PE) routers are configured with VPLS endpoint provisioning information that includes L2 VFI, VPN, and VPLS IDs. BGP neighbors are configured and activated under L2VPN address family to ensure that the VPLS endpoint provisioning information is saved to a separate L2VPN RIB and then distributed to other BGP peers in BGP update messages. When the endpoint information is received by the BGP peers, a pseudowire mesh is set up to support L2VPN-based services.

Router A

```
enable
configure terminal
l2 vfi customerA autodiscovery
 vpn id 100
 vpls-id 45000:100
 exit
l2 vfi customerB autodiscovery
 vpn id 200
 vpls-id 45000:200
 exit
router bgp 45000
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 172.16.1.2 remote-as 45000
 neighbor 172.21.1.2 remote-as 45000
 address-family l2vpn vpls
 neighbor 172.16.1.2 activate
 neighbor 172.16.1.2 send-community extended
 neighbor 172.21.1.2 activate
 neighbor 172.21.1.2 send-community extended
 end
```

Router B

```
enable
configure terminal
l2 vfi customerA autodiscovery
 vpn id 100
 vpls-id 45000:100
 exit
l2 vfi customerB autodiscovery
 vpn id 200
 vpls-id 45000:200
 exit
router bgp 45000
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 172.16.1.1 remote-as 45000
 neighbor 172.22.1.1 remote-as 45000
```

```
address-family l2vpn vpls
neighbor 172.16.1.1 activate
neighbor 172.16.1.1 send-community extended
neighbor 172.22.1.1 activate
neighbor 172.22.1.1 send-community extended
end
```

Related Commands

Command	Description
neighbor activate	Enables the exchange of information with a BGP neighboring router.
show ip bgp l2vpn	Displays L2VPN address family information.

address-family mvpn

To enter address family configuration mode to configure a routing session using multicast VPN (MVPN) address information, use the **address-family mvpn** command in router configuration mode. To exit address family configuration mode and remove the MVPN address family configuration from the running configuration, use the **no** form of this command.

address-family {**ipv4** | **ipv6**} **mvpn** [{**vrf** *vrf-name*}]
no address-family {**ipv4** | **ipv6**} **mvpn** [{**vrf** *vrf-name*}]

Syntax Description

ipv4	Specifies IPv4 MVPN address prefixes.
ipv6	Specifies IPv6 MVPN address prefixes.
vrf *vrf-name*	(Optional) Specifies the name of the VPN routing and forwarding (VRF) instance to associate with subsequent address family configuration mode commands.

Command Default

MVPN address prefixes are not configured

Command Modes

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.

Usage Guidelines

The **address-family mvpn** command places the router in address family configuration mode (prompt: config-router-af), from which you can configure routing sessions that use MVPN address information. To leave address family configuration mode and return to router configuration mode, type **exit**.

Configure **address-family ipv4 mvpn** to enable IPv4 multicast customer-route (c-route) exchange.

Configure **address-family ipv6 mvpn** to enable IPv6 multicast c-route exchange.

Examples

The following example places the device in address family configuration mode for IPv4 MVPN address prefixes:

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

Related Commands

Command	Description
address-family ipv4 (BGP)	Configures a routing session using standard IPv4 address prefixes.

address-family nsap

To enter address family configuration mode to configure Connectionless Network Service (CLNS)-specific parameters for Border Gateway Protocol (BGP) routing sessions, use the **address-family nsap** command in router configuration mode. To exit address family configuration mode and remove the CLNS address family configuration from the running configuration, use the **no** form of this command.

address-family nsap [**unicast**]
no address-family nsap [**unicast**]

Syntax Description

unicast	(Optional) Specifies network service access point (NSAP) unicast address prefixes.

Command Default

NSAP prefix support is not enabled.

Note Routing information for address family IPv4 is advertised by default for each BGP routing session configured with the **neighbor remote-as** command unless you configure the **no bgp default ipv4-unicast** command before configuring the **neighbor remote-as** command.

Command Modes

Router configuration (config-router)

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 **address-family nsap** command enters address family configuration mode (prompt: config-router-af)#, from which you can configure routing sessions that use standard NSAP address prefixes; you must enter NSAP address family configuration mode to configure BGP for CLNS prefixes.

To leave address family configuration mode and return to router configuration mode without removing the existing configuration, enter the **exit-address-family** command.

Examples

The following example enters NSAP address family configuration mode under BGP:

```
Router(config)# router bgp 50000
Router(config-router)# address-family nsap
Router(config-router-af)#
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Enters address family configuration mode for configuring routing sessions, such as BGP, that use standard IPv4 address prefixes.
address-family ipv6	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard IPv6 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPN Version 4 address prefixes.
bgp default ipv4-unicast	Enables the IPv4 unicast address family on all neighbors.
neighbor activate	Enables the exchange of information with a BGP neighboring router.

address-family rtfilter unicast

To enter address family configuration mode and to enable Route Target Constrain (RTC) with a Border Gateway Protocol (BGP) peer, use the **address-family rtfilter unicast** command in router configuration mode. To remove RTC, use the **no** form of the command.

address-family rtfilter unicast
no address-family rtfilter unicast

Syntax Description

This command has no arguments or keywords.

Command Default

No RTC support is enabled for BGP.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
15.1(1)S	This command was introduced.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use this command when you are configuring the BGP: RT Constrained Route Distribution feature.

The **address-family rtfilter unicast** command is configured on the provider edge (PE) and route reflector (RR). The command enables the PE to send RTC Network Layer Reachability Information (NLRI) to an RR. As soon as you configure a peer as a RR client, the default filter and default route are sent out also.

Examples

In the following example, the local PE is configured to send RTC NLRI to the neighboring RR at 10.2.2.2:

```
router bgp 65000
 address-family rtfilter unicast
 neighbor 10.2.2.2 activate
 neighbor 10.0.0.2 send-community extended
 exit-address-family
```

In the following example, the local PE is configured with the RTC default filter, which indicates that the PE wants all of the VPN routes (regardless of the RT values):

```
router bgp 65000
 address-family rtfilter unicast
 neighbor 10.2.2.2 activate
 neighbor 10.0.0.2 send-community extended
 neighbor 10.2.2.2 default-originate
 exit-address-family
```

In the following example, the RR is configured with the RTC default filter, which indicates that the RR is requesting the PE to advertise all of its routes to the RR:

```
router bgp 65000
 address-family rtfilter unicast
 neighbor 10.1.1.1 activate
 neighbor 10.1.1.1 route-reflector-client
 neighbor 10.1.1.1 default-originate
 exit-address-family
```

Related Commands

Command	Description
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.
router bgp	Configures the BGP routing process.
show ip bgp rtfilter	Displays information about BGP RT filtering.

address-family vpnv4

To enter address family configuration mode to configure a routing session using Virtual Private Network (VPN) Version 4 address prefixes, use the **address-family vpnv4** command in router configuration mode. To exit address family configuration mode and remove the VPNv4 address family configuration from the running configuration, use the **no** form of this command.

address-family vpnv4 [**multicast** | **unicast**]
no address-family vpnv4 [**multicast** | **unicast**]

Syntax Description

multicast	(Optional) Specifies VPN Version 4 multicast address prefixes.
unicast	(Optional) Specifies VPN Version 4 unicast address prefixes.

Command Default

Unicast prefix support is enabled by default when this command is entered without any optional keywords.

Note Routing information for address family IPv4 is advertised by default for each Border Gateway Protocol (BGP) routing session configured with the **neighbor remote-as** command unless you configure the **no bgp default ipv4-unicast** command before configuring the **neighbor remote-as** command.

Command Modes

Router configuration (config-router)

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.
Cisco IOS XE Release 3.6S	This command was modified. Support for multicast VPN Version 4 was added.
15.2(4)S	This command was implemented on the Cisco 7200 series router.

Usage Guidelines

The **address-family vpnv4** command replaces the **match nlri** and **set nlri** commands.

The **address-family vpnv4** command places the router in address family configuration mode (prompt: config-router-af), from which you can configure routing sessions that use VPN Version 4 address prefixes.

To leave address family configuration mode and return to router configuration mode without removing the existing configuration, enter the **exit-address-family** command.

Examples

The following example places the router in address family configuration mode for the VPN Version 4 address family:

```
Router(config)# router bgp 50000
Router(config-router)# address-family vpnv4
Router(config-router-af)#
```

The following example places the router in address family configuration mode for the unicast VPN Version 4 address family:

```
Router(config)# router bgp 50000
Router(config-router)# address-family vpnv4 unicast
Router(config-router-af)#
```

The following example places the router in address family configuration mode for the multicast VPN Version 4 address family:

```
Router(config)# router bgp 50000
Router(config-router)# address-family vpnv4 multicast
Router(config-router-af)#
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IP Version 4 address prefixes.
address-family ipv6	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard IPv6 address prefixes.
address-family nsap	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use CLNS prefixes.
exit-address-family	Exits the address family configuration mode and returns to router configuration mode without removing the existing configuration
neighbor activate	Enables the exchange of information with a BGP neighboring router.

advertise additional-paths

To advertise additional paths for a BGP peer policy template based on selection, use the **advertise additional-paths** command in peer policy template configuration mode. To prevent the advertisement of additional paths for a peer policy template, use the **no** form of the command.

advertise additional-paths [**best** *number*] [**group-best**] [**all**]
no advertise additional-paths [**best** *number*] [**group-best**] [**all**]

Syntax Description

best *number*	(Optional) Advertises the paths tagged with the **best 2** or **best 3** tag.
group-best	(Optional) Advertises the set of paths tagged with the **group-best** tag.
all	(Optional) Advertises paths tagged with the **all** tag.

Command Default

This command has no default behavior.

Command Modes

Peer policy template (config-router-ptmp)

Command History

Release	Modification
15.2(4)S	This command was introduced.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.
15.3(1)T	This command was integrated into Cisco IOS Release 15.3(1)T.

Usage Guidelines

Use this command to specify for the peer policy template which additional paths are advertised. You can advertise additional paths based on any combination of the selection methods, but you must choose at least one selection method if you use this command.

Keep in mind that in order to advertise additional-paths, you also need to:

- Configure the additional-path send capability, and that send capability must be negotiated (other than best-path).
- Select paths (other than best-path) with the **bgp additional-paths select** command, which sets the tags.

Examples

In the following example, a peer policy template named rr-client-pt1 is configured with the additional path sending and receiving capability. The group-best and best 3 selection policies are configured, and paths tagged with the best 3 tag are advertised.

```
router bgp 45000
address-family ipv4 unicast
 bgp additional-paths send receive
 bgp additional-paths select group-best best 3
 template peer-policy rr-client-pt1
  additional-paths send receive
  advertise additional-paths best 3
  exit
 address-family ipv4 unicast
```

```
neighbor 192.168.1.1 remote-as 45000
neighbor 192.168.1.1 inherit peer-policy rr-client-pt1
end
```

Related Commands

Command	Description
additional-paths	Configures the send and receive capabilities of additional path information for a peer template.
bgp additional-paths select	Causes the system to calculate BGP additional paths that can be candidates for advertisement in addition to a bestpath.
neighbor advertise additional-paths	Advertises additional paths for a neighbor based on selection.
neighbor inherit peer-policy	Sends a peer policy template to a neighbor so that the neighbor can inherit the configuration.
show ip bgp	Displays information about BGP neighbors, including path selections and path IDs.
show ip bgp neighbors	Displays information about the TCP and BGP connections to neighbors.
template peer-policy	Creates a peer policy template.

aggregate-address

To create an aggregate entry in a Border Gateway Protocol (BGP) database, use the **aggregate-address** command in address family or router configuration mode. To disable this function, use the **no** form of this command.

aggregate-address *address mask* [**as-set**] [**as-confed-set**] [**summary-only**] [**suppress-map** *map-name*] [**advertise-map** *map-name*] [**attribute-map** *map-name*]
no aggregate-address *address mask* [**as-set**] [**as-confed-set**] [**summary-only**] [**suppress-map** *map-name*] [**advertise-map** *map-name*] [**attribute-map** *map-name*]

Syntax Description

address	Aggregate address.
mask	Aggregate mask.
as-set	(Optional) Generates autonomous system set path information.
as-confed-set	(Optional) Generates autonomous confederation set path information.
summary-only	(Optional) Filters all more-specific routes from updates.
suppress-map *map-name*	(Optional) Specifies the name of the route map used to select the routes to be suppressed.
advertise-map *map-name*	(Optional) Specifies the name of the route map used to select the routes to create AS_SET origin communities.
attribute-map *map-name*	(Optional) Specifies the name of the route map used to set the attribute of the aggregate route.

Command Default

The atomic aggregate attribute is set automatically when an aggregate route is created with this command unless the **as-set** keyword is specified.

Command Modes

Address family configuration (config-router-af)

Router configuration (config-router)

Command History

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

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	Support for IPv6 was added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
12.2(33)SRE	The **as-confed-set** keyword was added.
Cisco IOS XE Release 3.1S	This command was introduced on Cisco ASR 1000 series routers.

Usage Guidelines

You can implement aggregate routing in BGP and Multiprotocol BGP (mBGP) either by redistributing an aggregate route into BGP or mBGP, or by using the conditional aggregate routing feature. In method of route aggregation, a route towards Null0 inserted into RIB automatically to help prevent forwarding loops caused by aggregation.

Using the **aggregate-address**command with no keywords will create an aggregate entry in the BGP or mBGP routing table if any more-specific BGP or mBGP routes are available that fall within the specified range. (A longer prefix that matches the aggregate must exist in the Routing Information Base (RIB).) The aggregate route will be advertised as coming from your autonomous system and will have the atomic aggregate attribute set to show that information might be missing. (By default, the atomic aggregate attribute is set unless you specify the **as-set** keyword.)

Using the **as-set**keyword creates an aggregate entry using the same rules that the command follows without this keyword, but the path advertised for this route will be an AS_SET consisting of all elements contained in all paths that are being summarized. Do not use this form of the **aggregate-address**commandwhen aggregating many paths, because this route must be continually withdrawn and updated as autonomous system path reachability information for the summarized routes changes.

Using the **as-confed-set** keyword creates an aggregate entry using the same rules that the command follows without this keyword. This keyword performs the same function as the **as-set** keyword, except that it generates autonomous confed set path information.

Using the **summary-only**keyword not only creates the aggregate route (for example, 192.*.*.*) but also suppresses advertisements of more-specific routes to all neighbors. If you want to suppress only advertisements to certain neighbors, you may use the **neighbor distribute-list** command, with caution. If a more-specific route leaks out, all BGP or mBGP routers will prefer that route over the less-specific aggregate you are generating (using longest-match routing).

Using the **suppress-map**keyword creates the aggregate route but suppresses advertisement of specified routes. You can use the **match** clauses of route maps to selectively suppress some more-specific routes of the aggregate and leave others unsuppressed. IP access lists and autonomous system path access lists match clauses are supported.

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

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

Examples

AS-Set Example

In the following example, an aggregate BGP address is created in router configuration mode. The path advertised for this route will be an AS_SET consisting of all elements contained in all paths that are being summarized.

```
Router(config)# router bgp 50000
Router(config-router)# aggregate-address 10.0.0.0 255.0.0.0 as-set
```

Summary-Only Example

In the following example, an aggregate BGP address is created in address family configuration mode and applied to the multicast database under the IP Version 4 address family. Because the **summary-only** keyword is configured, more-specific routes are filtered from updates.

```
Router(config)# router bgp 50000
Router(config-router)# address-family ipv4 multicast
Router(config-router-af)# aggregate-address 10.0.0.0 255.0.0.0 summary-only
```

Conditional Aggregation Example

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

```
Router(config)# ip as-path access-list 1 deny ^1234_
Router(config)# ip as-path access-list 1 permit .*
Router(config)# !
Router(config)# route-map MAP-ONE
Router(config-route-map)# match ip as-path 1
Router(config-route-map)# exit
Router(config)# router bgp 50000
Router(config-router)# address-family ipv4
Router(config-router-af)# aggregate-address 10.0.0.0 255.0.0.0 as-set advertise-map
MAP-ONE
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.
ip as-path access-list	Defines a BGP autonomous system path access list.

Command	Description
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
neighbor distribute-list	Distributes BGP neighbor information in an access list.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.

aigp

To enable sending and receiving of the accumulated interior gateway protocol (AIGP) attribute per external Border Gateway Protocol (eBGP) and internal Border Gateway Protocol (iBGP) neighbors, use the **aigp** command in address family configuration mode. To disable this functionality, use the **no** form of this command.

aigp
no aigp

Syntax Description

This command has no arguments or keywords.

Command Default

AIGP is disabled for iBGP and eBGP.

Command Modes

Address family configuration (config-router-af)

Command History

Release	Modification
Cisco IOS XE Release 3.12S	This command was introduced.
15.4(2)S	This command was integrated into Cisco IOS Release 15.4(2)S.

Usage Guidelines

Use the **aigp** command to enable sending and receiving of the AIGP attribute per neighbor.

This command is supported in the following address families:

- IPv4 unicast
- IPv4 multicast
- IPv6 unicast
- IPv6 multicast

Examples

The following example shows how to enable AIGP send and receive capability in address family configuration mode:

```
Device# configure terminal
Device(config)# router bgp 65000
Device(config-router)# address-family ipv4 unicast
Device(config-router-af)# neighbor 10.1.1.1 aigp
Device(config-router-af)# exit
```

Related Commands

Command	Description
neighbor aigp send cost-community	Converts AIGP to the cost community on the send side.
neighbor aigp send med	Converts AIGP to the multi-exit discriminator (MED) on the send side.

autodiscovery (MPLS)

To designate a Layer 2 virtual forwarding interface (VFI) as having Border Gateway Protocol (BGP) or Label Distribution Protocol (LDP) autodiscovered pseudowire members, use the **autodiscovery** command in L2 VFI configuration mode. To disable autodiscovery, use the **no** form of this command.

autodiscovery bgp signaling {**bgp** | **ldp**}[{**template** *template-name*}]
no autodiscovery bgp signaling {**bgp** | **ldp**}[{**template** *template-name*}]

Syntax Description

bgp	Specifies that BGP should be used for signaling and autodiscovery.
ldp	Specifies that LDP should be used for signaling.
template *template-name*	Specifies the template to be used for autodiscovered pseudowires.

Command Default

Layer 2 VFI autodiscovery is disabled.

Command Modes

L2 VFI configuration (config-vfi)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced as part of the Multiprotocol Label Switching (MPLS)-based L2VPN command modifications for cross-OS support.. This command will replace the **l2 vfi autodiscovery** command in future releases.
Cisco IOS XE Release 3.8S	This command was modified. The **bgp** keyword was added.
15.3(1)S	This command was integrated in Cisco IOS Release 15.3(1)S.

Usage Guidelines

This command was introduced as part of the Multiprotocol Label Switching (MPLS)-based L2VPN command modifications for cross-OS support. This command will replace the **l2 vfi autodiscovery** command in future releases.

Layer 2 VFI autodiscovery enables each VPLS PE router to discover other PE routers that are part of the same VPLS domain. VPLS autodiscovery also automatically detects when PE routers are added to or removed from the VPLS domain

The **bgp** keyword specifies that BGP should be used for signaling and autodiscovery, accordance with RFC 4761.

The **ldp** keyword specifies that LDP should be used for signaling. BGP will be used for autodiscovery.

Use of the **autodiscovery** command places the device into L2VPN VFI autodiscovery configuration mode (config-vfi-autodiscovery).

Examples

The following example shows how to enable Layer 2 VFI as having BGP autodiscovered pseudowire members and specify that LDP signaling should be used for autodiscovery:

```
Device(config)# l2vpn vfi context vfi1
Device(config-vfi)# vpn id 100
```

```
Device(config-vfi)# autodiscovery bgp signaling ldp
Device(config-vfi-autodiscovery)#
```

Related Commands

Command	Description
l2 vfi autodiscovery	Enables the VPLS PE router to automatically discover other PE routers that are part of the same VPLS domain.
vpn id	Sets or updates a VPN ID on a VPLS instance.

auto-summary (BGP)

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

auto-summary
no auto-summary

Syntax Description

This command has no arguments or keywords.

Command Default

Automatic summarization is disabled by default (the software sends subprefix routing information across classful network boundaries).

Command Modes

Address family configuration (config-router-af)

Router configuration (config-router)

Command History

Release	Modification
10.0	This command was introduced.
12.0(7)T	Address family configuration mode support was added.
12.2(8)T	The command default behavior was changed to disabled.
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.
15.0M, 12.2SRE	This command was modified. When an interface addressed with an address falling within the summarized range is shut down, that route no longer appears in the BGP routing table.

Usage Guidelines

BGP automatically summarizes routes to classful network boundaries when this command is enabled. Route summarization is used to reduce the amount of routing information in routing tables. Automatic summarization applies to connected, static, and redistributed routes.

Note The MPLS VPN Per VRF Label feature does not support auto-summary.

By default, automatic summarization is disabled and BGP accepts subnets redistributed from an Interior Gateway Protocol (IGP). To block subnets and create summary subprefixes to the classful network boundary when crossing classful network boundaries, use the **auto-summary** command.

To advertise and carry subnet routes in BGP when automatic summarization is enabled, use an explicit **network** command to advertise the subnet. The **auto-summary**command does not apply to routes injected into BGP via the **network** command or through iBGP or eBGP.

Why auto-summary for BGP Is Disabled By Default

When **auto-summary** is enabled, routes injected into BGP via redistribution are summarized on a classful boundary. Remember that a 32-bit IP address consists of a network address and a host address. The subnet mask determines the number of bits used for the network address and the number of bits used for the host address. The IP address classes have a natural or standard subnet mask, as shown in the table below.

Table 1: IP Address Classes

Class	Address Range	Standard Mask
A	1.0.0.0 to 126.0.0.0	255.0.0.0 or /8
B	128.1.0.0 to 191.254.0.0	255.255.0.0 or /16
C	192.0.1.0 to 223.255.254.0	255.255.255.0 or /24

Reserved addresses include 128.0.0.0, 191.255.0.0, 192.0.0.0, and 223.255.255.0.

When using the standard subnet mask, Class A addresses have one octet for the network, Class B addresses have two octets for the network, and Class C addresses have three octets for the network.

Consider the Class B address 156.26.32.1 with a 24-bit subnet mask, for example. The 24-bit subnet mask selects three octets, 156.26.32, for the network. The last octet is the host address. If the network 156.26.32.1/24 is learned via an IGP and is then redistributed into BGP, if **auto-summary** were enabled, the network would be automatically summarized to the natural mask for a Class B network. The network that BGP would advertise is 156.26.0.0/16. BGP would be advertising that it can reach the entire Class B address space from 156.26.0.0 to 156.26.255.255. If the only network that can be reached via the BGP router is 156.26.32.0/24, BGP would be advertising 254 networks that cannot be reached via this router. This is why the **auto-summary (BGP)**command is disabled by default.

Examples

In the following example, automatic summarization is enabled for IPv4 address family prefixes:

```
Router(config)# router bgp 50000

Router(config-router)# address-family ipv4 unicast

Router(config-router-af)# auto-summary

Router(config-router-af)# network 7.7.7.7 255.255.255.255
```

In the example, there are different subnets, such as 7.7.7.6 and 7.7.7.7 on Loopback interface 6 and Loopback interface 7, respectively. Both **auto-summary** and a **network** command are configured.

```
Router# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Ethernet0/0            100.0.1.7       YES NVRAM  up                    up
Ethernet0/1            unassigned      YES NVRAM  administratively down down
Ethernet0/2            unassigned      YES NVRAM  administratively down down
Ethernet0/3            unassigned      YES NVRAM  administratively down down
Ethernet1/0            108.7.9.7       YES NVRAM  up                    up
Ethernet1/1            unassigned      YES NVRAM  administratively down down
Ethernet1/2            unassigned      YES NVRAM  administratively down down
Ethernet1/3            unassigned      YES NVRAM  administratively down down
Loopback6              7.7.7.6         YES NVRAM  up                    up
Loopback7              7.7.7.7         YES NVRAM  up                    up
```

Note that in the output below, because of the **auto-summary** command, the BGP routing table displays the summarized route 7.0.0.0 instead of 7.7.7.6. The 7.7.7.7/32 network is displayed because it was configured with the **network** command, which is not affected by the **auto-summary** command.

```
Router# show ip bgp
BGP table version is 10, local router ID is 7.7.7.7
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 6.6.6.6/32       100.0.1.6                0             0 6 i
*> 7.0.0.0          0.0.0.0                  0         32768 ?   <-- summarization
*> 7.7.7.7/32       0.0.0.0                  0         32768 i   <-- network command
r>i9.9.9.9/32       108.7.9.9                0    100      0 i
*> 100.0.0.0        0.0.0.0                  0         32768 ?
r> 100.0.1.0/24     100.0.1.6                0             0 6 ?
*> 108.0.0.0        0.0.0.0                  0         32768 ?
r>i108.7.9.0/24     108.7.9.9                0    100      0 ?
*>i200.0.1.0        108.7.9.9
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
network (BGP and multiprotocol BGP)	Specifies the networks to be advertised by BGP and multiprotocol BGP.

bgp additional-paths

To configure BGP to send or receive additional paths (for all neighbors in the address family), use the **bgp additional-paths** command in address family configuration mode. To disable the sending or receiving of additional-path capability for the address family, use the **no** form of this command.

bgp additional-paths {**send** [**receive**] | **receive** | **disable**}
no bgp additional-paths {**send** [**receive**] | **receive**}

Syntax Description

send	(Optional) Enables BGP to send additional paths to all neighbors in the address family.
receive	(Optional) Enables BGP to receive additional paths from all neighbors in the address family.
disable	(Optional) Overrides and disables the address family-wide command for the current template. Note that the **disable** keyword is mutually exclusive with the **send** and **receive** keywords.

Command Default

No additional paths are sent or received per address family.

Command Modes

Address family configuration (config-router-af)

Command History

Release	Modification
15.2(4)S	This command was introduced.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.
15.3(1)T	This command was integrated into Cisco IOS Release 15.3(1)T.

Usage Guidelines

Using this command will enable the sending and receiving of additional path capability for an address family, after successful negotiation with a neighbor. The ability to send and receive additional paths is negotiated between two BGP neighbors during session establishment. The following address families are supported: IPv4 unicast, IPv4 multicast, IPv4 unicast + label, IPv6 unicast, IPpv6 multicast, and IPv6 multicast + label.

The **bgp additional-paths** command controls whether the local device can send or receive additional paths to and from all neighbors within an address family. If the **neighbor additional-paths** command is configured, its send and receive configurations for that neighbor or peer group override the configuration for the address family.

When the additional paths feature is used with IPv4+label or IPv6+label, only one label is allocated.

Use the **show ip bgp neighbors** command to display whether neighbors are capable of sending or receiving additional paths. Use the **show ip bgp** command with a network address to display the path selections, path IDs, and the capabilities for advertising and receiving additional paths.

When **bgp additional-paths** is configured, that configuration is applied to all neighbors in that address family.

- If you want to disable additional paths for the address family, use the **no bgp additional-paths {send [receive] | receive}** command.
- If you want to disable additional paths for one of the neighbors, use the **neighbor additional-paths disable** command.

Examples

In the following example, BGP negotiates with each neighbor in the IPv6 multicast address family that it can send and receive additional paths:

```
router bgp 65000
 address-family ipv6 multicast
 bgp additional-paths send receive
```

In the following example, BGP negotiates with each neighbor in the IPv4 unicast address family that it can send additional paths:

```
router bgp 65000
 address-family ipv4 unicast
 bgp additional-paths send
```

In the following example, BGP negotiates with all neighbors in the IPv6 multicast address family that it can receive additional paths:

```
router bgp 65000
 address-family ipv6 multicast
 bgp additional-paths receive
```

In the following example, the send and receive capability of the neighbor overrides the receive-only capability of the address family:

```
router bgp 65000
 address-family ipv6 multicast
 bgp additional-paths receive
 bgp additional-paths select group-best
 neighbor 2001:DB8::1037 activate
 neighbor 2001:DB8::1037 additional-paths send receive
 neighbor 2001:DB8::1037 advertise additional-paths group-best
 neighbor 2001:DB8::1037 route-map add_path4 out
!
route-map add_path4 permit 10
 match additional-paths advertise-set group-best
 set metric 565
!
```

In the following example, BGP is prevented from sending additional paths to or receiving additional paths from all neighbors in the IPv6 unicast address family. Note that the **no bgp additional-paths send receive** command will not actually appear in the configuration file; this example shows the CLI commands entered by the user.

```
Device(config)# router bgp 65000
 Device(config-router)# address-family ipv6 unicast
 Device(config-router-af)# no bgp additional-paths send receive
```

Related Commands

Command	Description
additional-paths	Uses a policy template to configure BGP to send or receive additional paths.
advertise additional-paths	Advertise additional paths for a BGP peer policy template based on selection.
bgp additional-paths select	Causes the system to calculate BGP additional paths that can be candidates for advertisement in addition to a bestpath.
neighbor additional-paths	Configures the local device with the ability to send and receive additional path information to and from a neighbor or peer group.

Command	Description
neighbor advertise additional-paths	Advertises additional paths for a neighbor based on selection.
show ip bgp	Displays information about BGP networks, including path selections and path IDs.
show ip bgp neighbors	Displays information about the TCP and BGP connections to neighbors.

bgp additional-paths install

To enable Border Gateway Protocol (BGP) to calculate a backup path for a given address family and to install it into the Routing Information Base (RIB) and Cisco Express Forwarding, use the **bgp additional-paths install** command in address family configuration or router configuration mode. To remove the backup paths, use the **no** form of this command.

bgp additional-paths install
no bgp additional-paths install

Syntax Description

This command has no arguments or keywords.

Command Default

A backup path is not created.

Command Modes

Address family configuration (config-router-af)

Router configuration (config-router)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.
Cisco IOS XE Release 3.3S	Support for IPv6 address family configuration mode was added.
15.1(2)S	Support for IPv6 address family configuration mode was added.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

You can issue the **bgp additional-paths install** command in different modes, each of which protects VRFs in its own way:

- VPNv4 address family configuration mode protects all VRFs.
- IPv4 address family configuration mode protects only IPv4 VRFs.
- IPv6 address family configuration mode protects only IPv6 VRFs.
- Router configuration mode protects VRFs in the global routing table.

Examples

The following example shows how to calculate a backup path and install it into the RIB and Cisco Express Forwarding:

```
Router(config-router-af)# bgp additional-paths install
```

Related Commands

Command	Description
address-family ipv6	Enters address family configuration mode for configuring routing sessions such as BGP that use standard IPv6 address prefixes.
bgp advertise-best-external	Enables BGP to use an external route as the backup path after a link or node failure.

bgp additional-paths select (additional paths)

To have the system calculate BGP additional paths that can be candidates for advertisement in addition to a bestpath, use the **bgp additional-paths select** command in address family configuration mode. To remove this mechanism for calculating additional paths and diverse path, use the **no** form of the command.

bgp additional-paths select [**best** *number*] [**group-best**] [**all**]
no bgp additional-paths select [**best** *number*] [**group-best**] [**all**]

Syntax Description

best *number*	(Optional) Calculates 2 or 3 bestpaths. • The value of *number* can be 2 or 3. • The bestpath is included as one of the 2 or 3 additional paths. • Paths with a unique next hop are selected; paths with a duplicate next hop are not considered.
group-best	(Optional) Selects the set of paths that are the best paths from the paths of the same AS. • For example, suppose there are three autonomous systems: AS 100, 200, and 300. Paths p101, p102, and p103 are from AS 100; p201, p202, and p203 are from AS200; and p301, p302, and p303 are from AS300. If the BGP bestpath algorithm is run on the paths from each AS, the algorithm will select one bestpath from each set of paths from that AS. Assume p101 is the best from AS100, p201 is the best from AS200, and p301 is the best from AS300; then the **group-best** is the set of p101, p201, and p301. • Paths with a unique next hop are selected; paths with a duplicate next hop are not considered.
all	(Optional) Selects all paths. • Paths with a unique next hop are selected; paths with a duplicate next hop are not considered.

Command Default

No additional paths are selected to be advertised.

Command Modes

Address family configuration (config-router-af)

Command History

Release	Modification
15.2(4)S	This command was introduced.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.
15.3(1)T	This command was integrated into Cisco IOS Release 15.3(1)T.

Usage Guidelines

This command configures part of the BGP Additional Paths feature. This feature allows you to calculate multiple paths for the same prefix without the new paths implicitly replacing any previous paths. Use this command to select which paths are candidates as additional paths to be advertised to BGP peers.

You can specify any combination of the keywords in the same instance of the **bgp additional-paths select** command; you must specify at least one keyword.

In order to enable the BGP Additional Paths feature and have a reason for selecting which paths will be advertised, you must have the additional path Send capability specified and it must be negotiated (other than best-path).

After you have selected which additional paths are candidates for advertisement, you typically use the **neighbor advertise additional-paths** command to advertise the additional paths to a specific neighbor. Alternatively, you could use the **advertise additional-paths** command under the **template peer-policy** command to advertise the additional paths to BGP peers in the peer policy template.

Note The **bgp additional-paths select backup** and **bgp additional-paths select best-external** commands are for the diverse path feature, not the Additional Paths feature. If the diverse path feature is also configured, it will apply only to neighbors where additional path capability is not negotiated.

You can remove every selection option configured by issuing the **no bgp additional-paths select** command.

Note The **no bgp additional-paths select** command will remove anything configured after the **select** keyword, which means that it will remove diverse path configurations: **bgp additional-paths select backup** and **bgp additional-paths select best-external**, and additional path configurations: **bgp additional-paths select best** *number*, **bgp additional-paths select group-best**, and **bgp additional-paths select all**.

Examples

In the following example, there are one or more eBGP neighbors not shown in the configuration. The eBGP routes learned from these neighbors are advertised for the neighbors shown in the configuration, and their attributes are changed. The route map called add_path3 specifies that any path that is tagged with the **group-best** tag will have its metric set to 825 and will be advertised toward neighbor 2001:DB8::1045.

```
router bgp 1
 neighbor 2001:DB8::1045 remote-as 1
 neighbor 2001:DB8::1037 remote-as 1
!
 address-family ipv6 unicast
  bgp additional-paths send receive
  bgp additional-paths select group-best
  neighbor 2001:DB8::1045 activate
  neighbor 2001:DB8::1045 route-map add_path3 out
  neighbor 2001:DB8::1045 advertise additional-paths group-best
  exit-address-family
!
route-map add_path3 permit 10
 match additional-paths advertise-set group-best
 set metric 825
```

Related Commands

Command	Description
additional-paths	Uses a policy template to configure BGP to send or receive additional paths.

Command	Description
advertise additional-paths	Advertises additional paths for a BGP peer policy template based on selection.
bgp additional-paths	Configures BGP to send or receive additional paths per address family.
bgp additional-paths select (diverse path)	Calculates a second BGP bestpath.
neighbor additional-paths	Configures BGP to send or receive additional paths per neighbor.
neighbor advertise additional-paths	Configures BGP to advertise additional paths to the neighbor.
show ip bgp	Displays entries in the BGP routing table.
show ip bgp neighbors	Displays information about BGP and TCP connections to neighbors.

bgp additional-paths select (diverse path)

To have the system calculate a second Border Gateway Protocol (BGP) best path, use the **bgp additional-paths select** command in address family configuration mode. To remove this mechanism for calculating a second best path, use the **no** form of this command.

bgp additional-paths select {**best-external**[{**backup**}] | **backup**}
no bgp additional-paths select

Syntax Description

best-external	(Optional) Calculates a second best path from among those received from external neighbors. Configure this keyword on a provider edge (PE) or route reflector. This keyword enables the BGP Best External feature on a route reflector.
backup	(Optional) Calculates a second best path as a backup path.

Command Default

A second BGP best path is not calculated.

Command Modes

Address family configuration (config-router-af)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.

Usage Guidelines

The BGP Diverse Path feature can be enabled on a route reflector to calculate a best path and an additional path per address family.

Computation of a diverse path per address family is triggered by any of the following commands:

- **bgp additional-paths install**
- **bgp additional-paths select**
- **maximum-paths ebgp**
- **maximum-paths ibgp**

The **bgp additional-paths install** command will install the type of path that is specified in the **bgp additional-paths select** command. Either the **best-external** keyword or the **backup** keyword is required; both keywords can be specified. If both keywords (**best-external** and **backup**) are specified, the system will install a backup path.

Note The **bgp additional-paths select backup** and **bgp additional-paths select best-external** commands are for the Diverse Path feature, not the BGP Additional Paths feature. If the Diverse Path feature and the Additional Paths feature are configured, the Diverse Path feature will apply only to neighbors where additional path capability is not negotiated.

You can remove every selection option configured by issuing the **no bgp additional-paths select** command.

Note The **no bgp additional-paths select** command will remove anything configured after the **select** keyword, which means that it will remove diverse path configurations: **bgp additional-paths select backup** and **bgp additional-paths select best-external**, and additional path configurations: **bgp additional-paths select best** *number*, **bgp additional-paths select group-best**, and **bgp additional-paths select all**.

Examples

In the following example, the system computes a second best path from among those received from external neighbors:

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

Related Commands

Command	Description
bgp additional-paths install	Enables BGP to calculate a backup path for a given address and to install it into the RIB and CEF.
bgp bestpath igp-metric ignore	Specifies that the system ignore the IGP metric during best path selection.
maximum-paths ebgp	Configures multipath load sharing for EBGP and IBGP routes.
maximum-paths ibgp	Controls the maximum number of parallel IBGP routes that can be installed in a routing table.

bgp advertise-best-external

To enable Border Gateway Protocol (BGP) to calculate an external route as the best backup path for a given address family and to install it into the Routing Information base (RIB) and Cisco Express Forwarding, and to advertise the best external path to its neighbors, use the **bgp advertise-best-external** command in address family or router configuration mode. To remove the external backup path, use the **no** form of this command.

bgp advertise-best-external
no bgp advertise-best-external

Syntax Description

This command has no arguments or keywords.

Command Default

An external backup path is not created.

Command Modes

Router configuration (config-router)

Address family configuration (config-router-af)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.
Cisco IOS XE Release 3.3S	Support for IPv6 address family configuration mode was added.
15.1(2)S	Support for IPv6 address family configuration mode was added.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

When you configure the Best External feature with the **bgp advertise-best-external** command, you need not enable the Prefix Independent Convergence (PIC) feature with the **bgp additional-paths install** command. The Best External feature automatically installs a backup path. If you try to configure the PIC feature after configuring the Best External feature, you receive an error. This behavior applies to both BGP and MPLS.

When you configure the MPLS VPN: Best External feature with the **bgp advertise-best-external** command, it will override the functionality of the MPLS VPN--BGP Local Convergence feature. You need not remove the **protection local-prefixes** command from the configuration.

You can issue the **bgp advertise-best-external** command in different modes, each of which protects VRFs in its own way:

- VPNv4 address-family configuration mode protects all VRFs.
- IPv4 address-family configuration mode protects only IPv4 VRFs.
- IPv6 address family configuration mode protects only IPv6 VRFs.

- Router configuration mode protects VRFs in the global routing table.

Examples

The following example calculates an external backup path and installs it into the RIB and Cisco Express Forwarding:

```
Router(config-router-af)# bgp advertise-best-external
```

Related Commands

Command	Description
address-family ipv6	Enters address family configuration mode for configuring routing sessions such as BGP that use standard IPv6 address prefixes.
bgp additional-paths install	Enables BGP to use an additional path as the backup path.
protection local-prefixes	Enables PE-CE link protection by preserving the local label.

bgp aggregate-timer

To set the interval at which BGP routes will be aggregated or to disable timer-based route aggregation, use the **bgp aggregate-timer** command in address-family or router configuration mode. To restore the default value, use the **no** form of this command.

bgp aggregate-timer *seconds*
no bgp aggregate-timer

Syntax Description

seconds	Interval (in seconds) at which the system will aggregate BGP routes. • The range is from 6 to 60 or else 0 (zero). The default is 30. • A value of 0 (zero) disables timer-based aggregation and starts aggregation immediately.

Command Default

30 seconds

Command Modes

Address family configuration (config-router-af)

Router configuration (config-router)

Command History

Release	Modification
12.2SX	This command was introduced.
12.2M	This command was integrated into Cisco IOS Release 12.2 Mainline.
12.2SR	This command was integrated into Cisco IOS Release 12.2 SR.
XE 2.0	This command was integrated into Cisco IOS XE Release 2.0.
12.2(33)SRD4	The zero (0) timer was added.

Usage Guidelines

Use this command to change the default interval at which BGP routes are aggregated.

In very large configurations, even if the **aggregate-address summary-only** command is configured, more specific routes are advertised and later withdrawn. To avoid this behavior, configure the **bgp aggregate-timer** to 0 (zero), and the system will immediately check for aggregate routes and suppress specific routes.

Examples

The following example configures BGP route aggregation at 20-second intervals:

```
Router(config)# router bgp 50
Router(config-router)# bgp aggregate-timer 20
```

The following example starts BGP route aggregation immediately:

```
Router(config)# router bgp 50
Router(config-router)# aggregate-address 10.0.0.0 255.0.0.0 summary-only
Router(config-router)# bgp aggregate-timer 0
```

Related Commands

Command	Description
aggregate-address	Creates an aggregate entry in a BGP database.

bgp always-compare-med

To enable the comparison of the Multi Exit Discriminator (MED) for paths from neighbors in different autonomous systems, use the **bgp always-compare-med** command in router configuration mode. To disallow the comparison, use the **no** form of this command.

bgp always-compare-med
no bgp always-compare-med

Syntax Description

This command has no arguments or keywords.

Command Default

Cisco IOS software does not compare the MED for paths from neighbors in different autonomous systems if this command is not enabled or if the **no** form of this command is entered. The MED is compared only if the autonomous system path for the compared routes is identical.

Command Modes

Router configuration (config-router)

Command History

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

Usage Guidelines

The MED, as stated in RFC 1771, is an optional nontransitive attribute that is a four octet non-negative integer. The value of this attribute may be used by the BGP best path selection process to discriminate among multiple exit points to a neighboring autonomous system.

The MED is one of the parameters that is considered when selecting the best path among many alternative paths. The path with a lower MED is preferred over a path with a higher MED. During the best-path selection process, MED comparison is done only among paths from the same autonomous system. The **bgp always-compare-med** command is used to change this behavior by enforcing MED comparison between all paths, regardless of the autonomous system from which the paths are received.

The **bgp deterministic-med** command can be configured to enforce deterministic comparison of the MED value between all paths received from within the same autonomous system.

Examples

In the following example, the local BGP routing process is configured to compare the MED from alternative paths, regardless of the autonomous system from which the paths are received:

```
Router(config)# router bgp 500000

Router(config-router)# bgp always-compare-med
```

Related Commands

Command	Description
bgp deterministic-med	Enforces deterministic comparison of the MED value between all paths received from within the same autonomous system

bgp asnotation dot

To change the default display and regular expression match format of Border Gateway Protocol (BGP) 4-byte autonomous system numbers from asplain (decimal values) to dot notation, use the **bgp asnotation dot** command in router configuration mode. To reset the default 4-byte autonomous system number display and regular expression match format to asplain, use the **no** form of this command.

bgp asnotation dot
no bgp asnotation dot

Syntax Description

This command has no arguments or keywords.

Command Default

BGP autonomous system numbers are displayed using asplain (decimal value) format in screen output, and the default format for matching 4-byte autonomous system numbers in regular expressions is asplain.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
12.0(32)SY8	This command was introduced.
12.2(33)SXI1	This command was integrated into Cisco IOS Release 12.2(33)SXI1.
12.0(33)S3	This command was integrated into Cisco IOS Release 12.0(33)S3.
Cisco IOS XE Release 2.4	This command was integrated into Cisco IOS XE Release 2.4.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.
15.2(1)E	This command was integrated into Cisco IOS Release 15.2(1)E.

Usage Guidelines

Prior to January 2009, BGP autonomous system numbers that were allocated to companies were 2-octet numbers in the range from 1 to 65535 as described in RFC 4271, *A Border Gateway Protocol 4 (BGP-4)* . Due to increased demand for autonomous system numbers, the Internet Assigned Number Authority (IANA) will start in January 2009 to allocate four-octet autonomous system numbers in the range from 65536 to 4294967295. RFC 5396, *Textual Representation of Autonomous System (AS) Numbers* , documents three methods of representing autonomous system numbers. Cisco has implemented the following two methods:

- Asplain--Decimal value notation where both 2-byte and 4-byte autonomous system numbers are represented by their decimal value. For example, 65526 is a 2-byte autonomous system number and 234567 is a 4-byte autonomous system number.
- Asdot--Autonomous system dot notation where 2-byte autonomous system numbers are represented by their decimal value and 4-byte autonomous system numbers are represented by a dot notation. For

example, 65526 is a 2-byte autonomous system number and 1.169031 is a 4-byte autonomous system number (this is dot notation for the 234567 decimal number).

For details about the third method of representing autonomous system numbers, see RFC 5396.

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 as the default display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain and asdot format. In addition, the default format for matching 4-byte autonomous system numbers in regular expressions is asplain, so you must ensure that any regular expressions to match 4-byte autonomous system numbers are written in the asplain format. If you want to change the default **show** command output to display 4-byte autonomous system numbers in the asdot format, use the **bgp asnotation dot** command under router configuration mode. 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. The tables below show that although you can configure 4-byte autonomous system numbers in either asplain or asdot format, only one format is used to display **show** command output and control 4-byte autonomous system number matching for regular expressions, and the default is asplain format. To display 4-byte autonomous system numbers in **show** command output and to control matching for regular expressions in the asdot format, you must configure the **bgp asnotation dot** command. After enabling the **bgp asnotation dot** command, a hard reset must be initiated for all BGP sessions by entering the **clear ip bgp *** command.

Note If you are upgrading to an image that supports 4-byte autonomous system numbers, you can still use 2-byte autonomous system numbers. The **show** command output and regular expression match are not changed and remain in asplain (decimal value) format for 2-byte autonomous system numbers regardless of the format configured for 4-byte autonomous system numbers.

Table 2: Default Asplain 4-Byte Autonomous System Number Format

Format	Configuration Format	Show Command Output and Regular Expression Match Format
asplain	2-byte: 1 to 65535 4-byte: 65536 to 4294967295	2-byte: 1 to 65535 4-byte: 65536 to 4294967295
asdot	2-byte: 1 to 65535 4-byte: 1.0 to 65535.65535	2-byte: 1 to 65535 4-byte: 65536 to 4294967295

Table 3: Asdot 4-Byte Autonomous System Number Format

Format	Configuration Format	Show Command Output and Regular Expression Match Format
asplain	2-byte: 1 to 65535 4-byte: 65536 to 4294967295	2-byte: 1 to 65535 4-byte: 1.0 to 65535.65535
asdot	2-byte: 1 to 65535 4-byte: 1.0 to 65535.65535	2-byte: 1 to 65535 4-byte: 1.0 to 65535.65535

Examples

The following output from the **show ip bgp summary** command shows the default asplain format of the 4-byte autonomous system numbers. Note the asplain format of the 4-byte autonomous system numbers, 65536 and 65550.

```
Router# show ip bgp summary
BGP router identifier 172.17.1.99, local AS number 65538
BGP table version is 1, main routing table version 1
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  Statd
192.168.1.2     4        65536       7       7        1    0    0 00:03:04      0
192.168.3.2     4        65550       4       4        1    0    0 00:00:15      0
```

The following configuration is performed to change the default output format to the asdot notation format:

```
configure terminal
 router bgp 65538
  bgp asnotation dot
  end
clear ip bgp *
```

After the configuration is performed, the output is converted to asdot notation format as shown in the following output from the **show ip bgp summary** command. Note the asdot format of the 4-byte autonomous system numbers, 1.0 and 1.14 (these are the asdot conversions of the 65536 and 65550 autonomous system numbers).

```
Router# show ip bgp summary
BGP router identifier 172.17.1.99, local AS number 1.2
BGP table version is 1, main routing table version 1
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  Statd
192.168.1.2     4          1.0       9       9        1    0    0 00:04:13     0
192.168.3.2     4         1.14       6       6        1    0    0 00:01:24     0
```

After the **bgp asnotation dot** command is configured, the regular expression match format for 4-byte autonomous system paths is changed to asdot notation format. Although a 4-byte autonomous system number can be configured in a regular expression using either asplain format or asdot format, only 4-byte autonomous system numbers configured using the current default format are matched. In the first example, the **show ip bgp regexp**command is configured with a 4-byte autonomous system number in asplain format. The match fails because the default format is currently asdot format and there is no output. In the second example using asdot format, the match passes and the information about the 4-byte autonomous system path is shown using the asdot notation.

Note The asdot notation uses a period, which is a special character in Cisco regular expressions. To remove the special meaning, use a backslash before the period.

```
Router# show ip bgp regexp ^65536$
Router# show ip bgp regexp ^1\.0$
BGP table version is 2, local router ID is 172.17.1.99
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
*> 10.1.1.0/24      192.168.1.2              0             0 1.0 i
```

Related Commands

Command	Description
router bgp	Configures the BGP routing process.
show ip bgp regexp	Displays routes matching the autonomous system path regular expression.
show ip bgp summary	Displays the status of all BGP connections.

bgp bestpath aigp ignore

To configure a device that is running the Border Gateway Protocol (BGP) to not evaluate the accumulated interior gateway protocol (AIGP) attribute during the best path selection process between two paths when one path does not have the AIGP attribute, use the **bgp bestpath aigp ignore** command in router configuration mode. To return the device to default operation, use the **no** form of this command.

bgp bestpath aigp ignore
no bgp bestpath aigp ignore

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled by default until the AIGP attribute is manually configured.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Release 3.12S	This command was introduced.
15.4(2)S	This command was integrated into Cisco IOS Release 15.4(2)S.

Usage Guidelines

Use the **bgp bestpath aigp ignore** command to not evaluate the AIGP attribute during the best path selection process between two paths when one path does not have the AIGP attribute. When **bgp bestpath aigp ignore** is enabled, BGP does not use AIGP tie-breaking rules unless paths have the AIGP attribute.

Examples

The following example shows how to configure a device to not evaluate the AIGP attribute during the best path selection process:

```
Device# configure terminal
Device(config)# router bgp 50000
Device(config-router)# bgp bestpath aigp ignore
Device(config-router)# exit
```

Related Commands

Command	Description
aigp	Enables sending and receiving of the AIGP attribute per eBGP and iBGP neighbors.

bgp bestpath as-path ignore

To configure Border Gateway Protocol (BGP) to not consider the autonomous system (AS) path during best path route selection, use the **bgp bestpath as-path ignore** command in router configuration mode. To restore default behavior and configure BGP to consider the AS-path during route selection, use the **no** form of this command.

bgp bestpath as-path ignore
no bgp bestpath as-path ignore

Syntax Description

This command has no arguments or keywords.

Command Default

The AS-path is considered during BGP best path selection.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
12.0	This command was introduced.
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 BGP routing process is configured to not consider the AS-path during best path selection:

```
Router(config)# router bgp 40000
Router(config-router)# bgp bestpath as-path ignore
```

Related Commands

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

bgp bestpath compare-routerid

To configure a Border Gateway Protocol (BGP) routing process to compare identical routes received from different external peers during the best path selection process and to select the route with the lowest router ID as the best path, use the **bgp bestpath compare-routerid** command in router configuration mode. To return the BGP routing process to the default operation, use the **no** form of this command.

bgp bestpath compare-routerid
no bgp bestpath compare-routerid

Syntax Description

This command has no arguments or keywords.

Command Default

The behavior of this command is disabled by default; BGP selects the route that was received first when two routes with identical attributes are received.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
12.1(3)	This command was introduced.
12.0(11)S	This command was integrated into Cisco IOS Release 12.0(11)S.
12.1(3a)E	This command was integrated into Cisco IOS Release 12.1(3a)E.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **bgp bestpath compare-routerid** command is used to configure a BGP routing process to use the router ID as the tie breaker for best path selection when two identical routes are received from two different peers (all the attributes are the same except for the router ID). When this command is enabled, the lowest router ID will be selected as the best path when all other attributes are equal.

Examples

In the following example, the BGP routing process is configured to compare and use the router ID as a tie breaker for best path selection when identical paths are received from different peers:

```
Router(config)# router bgp 50000

Router(config-router)# bgp bestpath compare-routerid
```

Related Commands

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

bgp bestpath cost-community ignore

To configure a router that is running the Border Gateway Protocol (BGP) to not evaluate the cost community attribute during the best path selection process, use the **bgp bestpath cost-community ignore** command in router configuration mode. To return the router to default operation, use the **no** form of this command.

bgp bestpath cost-community ignore
no bgp bestpath cost-community ignore

Syntax Description

This command has no keywords or arguments.

Command Default

The behavior of this command is enabled by default until the cost community attribute is manually configured.

Command Modes

Address family configuration (config-router-af)

Router configuration (config-router)

Command History

Release	Modification
12.0(24)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.
12.2(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.

Usage Guidelines

The **bgp bestpath cost-community ignore** command is used to disable the evaluation of the cost community attribute to help isolate problems and troubleshoot issues that relate to BGP path selection. This command can also be used to delay the activation of cost community attribute evaluation so that cost community filtering can be deployed in a large network at the same time.

Examples

The following example shows how to configure a router to not evaluate the cost community attribute during the best path selection process:

```
router bgp 50000
 address-family ipv4 unicast
 bgp bestpath cost-community ignore
```

Related Commands

Command	Description
set extcommunity cost	Creates a set clause to apply the cost community attribute to routes that pass through a route map.
show ip bgp	Displays entries in the BGP routing table.

bgp bestpath igp-metric ignore

To specify that the system ignore the Interior Gateway Protocol (IGP) metric during Border Gateway Protocol (BGP) best path selection, use the **bgp bestpath igp-metric ignore** command in address family configuration mode. To remove the configuration to ignore the IGP metric, use the **no** form of this command.

bgp bestpath igp-metric ignore
no bgp bestpath igp-metric ignore

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

Address family configuration (config-router-af)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.

Usage Guidelines

The IGP metric is a configurable metric for EIGRP, IS-IS, or OSPF that is related to distance. The **bgp bestpath igp-metric ignore** command can be used independently or in conjunction with the BGP Diverse Path feature. This command does not enable the BGP Diverse Path feature.

Similarly, enabling the BGP Diverse Path feature does not necessarily require that the IGP metric be ignored. If you enable the BGP Diverse Path feature and the route reflector and its shadow route reflector are not colocated, this command must be configured on the route reflector, shadow route reflector, and provider edge (PE) routers.

This command is supported in the following address families:

- ipv4 unicast
- vpnv4 unicast
- ipv6 unicast
- vpnv6 unicast
- ipv4+label
- ipv6+label

Note This command is not supported per virtual routing and forwarding (VRF); if you use it per VRF, it is at your own risk.

This command applies per VRF as follows (which is consistent with the BGP PIC/Best External feature):

- When configured under the VPNv4 or VPNv6 address-family, it applies to all VRFs, but it will be nvgened only under VPNv4/VPNv6 global.
- When configured under a particular VRF, it applies only to that VRF and will be nvgened only for that VRF.
- When configured under vpnv4 or vpnv6 global, this command can be disabled for a particular VRF by specifying the **no bgp bestpath igp-metric ignore** command. The **no** form will be nvgened under that VRF, while under VPNv4 or VPNv6 the **bgp bestpath igp-metric ignore** command is nvgened and the command applies to all other VRFs.

Examples

In the following example, the IGP metric is ignored during calculation of the BGP best path:

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

Related Commands

Command	Description
bgp additional-paths select	Specifies that the system calculate a second BGP best path.

bgp bestpath med confed

To configure a Border Gateway Protocol (BGP) routing process to compare the Multi Exit Discriminator (MED) between paths learned from confederation peers, use the **bgp bestpath med confed** command in router configuration mode. To disable MED comparison of paths received from confederation peers, use the **no** form of this command.

bgp bestpath med confed [**missing-as-worst**]
no bgp bestpath med confed [**missing-as-worst**]

Syntax Description

missing-as-worst	(Optional) Assigns the value of infinity to received routes that do not carry the MED attribute, making these routes the least desirable.

Command Default

Cisco IOS software does not consider the MED attribute when choosing among paths learned from confederation peers if this command is not enabled or if the **no** form of this command is entered.

Command Modes

Router configuration (config-router)

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

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

path = 65000 65004, med = 2

path = 65001 65004, med = 3

path = 65002 65004, med = 4

path = 65003 1, med = 1

Examples

In the following example, the BGP routing process is configured to compare MED values for paths learned from confederation peers:

```
Router(config)# router bgp 50000

Router(config-router)# bgp bestpath med confed
```

Related Commands

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

bgp bestpath med missing-as-worst

To configure a Border Gateway Protocol (BGP) routing process to assign a value of infinity to routes that are missing the Multi Exit Discriminator (MED) attribute (making the path without a MED value the least desirable path), use the **bgp bestpath med missing-as-worst** command in router configuration mode. To return the router to the default behavior (assign a value of 0 to the missing MED), use the **no** form of this command.

bgp bestpath med missing-as-worst
no bgp bestpath med missing-as-worst

Syntax Description

This command has no arguments or keywords.

Command Default

Cisco IOS software assigns a value of 0 to routes the are missing the MED attribute, causing the route with the missing MED attribute to be considered the best path.

Command Modes

Router configuration (config-router)

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

In the following example, the BGP router process is configured to consider a route with a missing MED attribute as having a value of infinity (4294967294), making this path the least desirable path:

```
Router(config)# router bgp 50000

Router(config-router)# bgp bestpath med missing-as-worst
```

Related Commands

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

bgp bestpath prefix-validate

To disable the validation of Border Gateway Protocol (BGP) prefixes based on the autonomous system from which the prefix originates, or to allow invalid prefixes to be used as the bestpath even if valid prefixes are available, use the **bgp bestpath prefix-validate** command in router configuration mode or IPv4 or IPv6 address family configuration mode. To disable either behavior, use the **no** form of this command.

bgp bestpath prefix-validate {**disable** | **allow-invalid**}
no bgp bestpath prefix-validate {**disable** | **allow-invalid**}

Syntax Description

disable	Disables the checking of prefixes to see if they are valid and disables the storage of validation information.
allow-invalid	Allows invalid prefixes to be used as the bestpath, even if valid prefixes are available. • You might want to allow invalid prefixes so that a route map can set the local preference, metric, or other property to allow the use of an invalid prefix only when no other path is available.

Command Default

Invalid prefixes are allowed to be used as the best path.

Command Modes

Router configuration (config-router)

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

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.
15.2(1)S	This command was integrated into Cisco IOS Release 15.2(1)S.
15.2(4)S	This command was implemented on the Cisco 7200 series routers.

Usage Guidelines

This command is useful for configuration testing and for use with a route map.

The default behavior, if neither the **bgp bestpath prefix-validate disable** nor the **bgp bestpath prefix-validate allow-invalid** command is configured, is to prefer prefixes in the following order:

- Those with a validation state of valid
- Those with a validation state of not found
- Those with a validation state of invalid (which will never be installed in the routing table)

These preferences override metric, local-preference, and other choices made during the bestpath computation. The standard bestpath decision tree applies only if the two paths are the same.

If both the **bgp bestpath prefix-validate disable** command and the **bgp bestpath prefix-validate allow-invalid** command are configured, the **disable** command will prevent a validation state from being assigned to prefixes, so the **allow-invalid** command will have no effect.

Examples

The following example disables the checking of prefixes to see if they are valid, and disables the storage of validation information:

```
router bgp 65000
 address-family ipv4 unicast
 bgp bestpath prefix-validate disable
```

Related Commands

Command	Description
bgp rpki server	Connects to an RPKI server and enables the validation of BGP prefixes based on the AS from which the prefix originates.
clear ip bgp rpki server	Closes the TCP connection to the specified RPKI server, purges SOVC records downloaded from that server, renegotiates the connection, and redownloads SOVC records.
show ip bgp rpki servers	Displays the current state of communication with RPKI servers.
show ip bgp rpki table	Displays the currently cached list of networks and associated AS numbers received from the RPKI server.

bgp client-to-client reflection

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

bgp client-to-client reflection [**all**]
no bgp client-to-client reflection [**all**]

Syntax Description

all	(Optional) This keyword does nothing in the positive or negative form of the command. It is just to remind the network administrator that the command enables [or disables] both intercluster and intracluster client-to-client reflection.

Command Default

Client-to-client route reflection is enabled by default; when a route reflector is configured, the route reflector reflects routes from a client to other clients.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
11.1	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.
Cisco IOS XE Release 3.8S	This command was modified. The **all** keyword was added.

Usage Guidelines

This command affects route reflection of all routes, both intracluster and intercluster.

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

Note that the **bgp client-to-client reflection** command affects intracluster and intercluster client-to-client reflection, unlike the **bgp client-to-client reflection intra-cluster** command, which affects only intracluster (within a cluster) client-to-client route reflection.

There are three levels of configuration that can disable client-to-client reflection. The software performs them in the following order, from least specific to most specific:

1. Least specific: **no bgp client-to-client reflection [all]** Disables intracluster and intercluster client-to-client reflection.
2. More specific: **no bgp client-to-client reflection intra-cluster cluster-id any** Disables intracluster client-to-client reflection for any cluster-id.

3. Most specific: **no bgp client-to-client reflection intra-cluster cluster-id** *cluster-id1 cluster-id2 ...* Disables intracluster client-to-client reflection for the specified clusters.

When BGP is advertising updates, the software evaluates each level of configuration in order. Once any level of configuration disables client-to-client reflection, no further evaluation of more specific policies is necessary.

Note the results of the base (positive) and negative (**no**) forms of the three commands listed above:

- A negative configuration (that is, with the **no** keyword) overwrites any less specific configuration.
- A positive configuration (that is, without the **no** keyword) will lose out to (default to) what is configured in a less specific configuration.
- Configurations at any level appear in the configuration file only if they are negative.

Examples

In the following example, the local router is a route reflector, and the three neighbors are fully meshed. Because the neighbors are fully meshed, the network administrator disables both intracluster and intercluster client-to-client reflection by entering the **no** form of the command. The **no bgp client-to-client reflection** command affects all routes.

```
Device(config)# router bgp 50000
Device(config-router)# neighbor 10.24.95.22 route-reflector-client
Device(config-router)# neighbor 10.24.95.23 route-reflector-client
Device(config-router)# neighbor 10.24.95.24 route-reflector-client
Device(config-router)# no bgp client-to-client reflection
Device(config-router)# end
```

Related Commands

Command	Description
bgp client-to-client reflection intra-cluster	Enables or restores intracluster client-to-client route reflection to clients for the specified clusters.
bgp cluster-id	Sets the global cluster ID on a route reflector.
neighbor route-reflector-client	Configures the router as a BGP route reflector and configures the specified neighbor as its client.
show ip bgp cluster-ids	Displays cluster IDs, how many neighbors are in each cluster, and whether client-to-client route reflection has been disabled for each cluster.

bgp client-to-client reflection intra-cluster

To enable intracluster client-to-client route reflection to clients for the specified clusters, use the **bgp client-to-client reflection intra-cluster** command in router configuration mode. To disable intracluster client-to-client route reflection for the specified clusters, use the **no** form of this command.

bgp client-to-client reflection intra-cluster cluster-id {**any** | *cluster-id1* [*cluster-id2*] **. . .**}
no bgp client-to-client reflection intra-cluster cluster-id {**any** | *cluster-id1* [*cluster-id2*] **. . .**}

Syntax Description

cluster-id	Keyword that precedes the **any** keyword or the cluster IDs in the command.
any	Enables intracluster, client-to-client route reflection within any cluster configured on the route reflector.
cluster-id1	Cluster ID (specified by the **neighbor cluster-id** command) for which intracluster client-to-client route reflection is enabled. • At least one *cluster-id* is required, unless the **any** keyword is specified. • More than one *cluster-id* can be specified.

Command Default

Client-to-client route reflection is enabled by default; when a route reflector is configured, the route reflector reflects routes from a client to other clients.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.

Usage Guidelines

By default, the clients of a route reflector are not required to be fully meshed and the routes from a client are reflected to other clients. However, if the clients are fully meshed, route reflection is not required. In this case, use the **no bgp client-to-client reflection intra-cluster** command to disable client-to-client reflection; updates are not sent (reflected) because they are not necessary. Configure this command on a route reflector.

There are three levels of configuration that can disable client-to-client reflection. The software performs them in the following order, from least specific to most specific:

1. Least specific: **no bgp client-to-client reflection [all]** Disables intracluster and intercluster client-to-client reflection.
2. More specific: **no bgp client-to-client reflection intra-cluster cluster-id any** Disables intracluster client-to-client reflection for any cluster-id.
3. Most specific: **no bgp client-to-client reflection intra-cluster cluster-id** *cluster-id1 cluster-id2* ... Disables intracluster client-to-client reflection for the specified clusters.

When BGP is advertising updates, the software evaluates each level of configuration in order. Once any level of configuration disables client-to-client reflection, no further evaluation of more specific policies is necessary.

Note the results of the base (positive) and negative (**no**) forms of the three commands listed above:

- A negative configuration (that is, with the **no** keyword) overwrites any less specific configuration.
- A positive configuration (that is, without the **no** keyword) will lose out to (default to) what is configured in a less specific configuration.
- Configurations at any level appear in the configuration file only if they are negative.

All levels can be configured independently and all levels appear in the configuration file independently of the configuration of other levels.

Note that negative configuration makes any more specific configuration unnecessary (because even if the more specific configuration is positive, it is not processed after the negative configuration; if the more specific configuration is negative, it is functionally the same as the earlier negative configuration). The following examples illustrate this behavior.

Example 1

no bgp client-to-client reflection

no bgp client-to-client reflection intra-cluster cluster-id any

Intercluster and intracluster reflection are disabled (based on the first command). The second command disables intracluster reflection, but it is unnecessary because intracluster reflection is already disabled by the first command.

Example 2

no bgp client-to-client reflection intra-cluster cluster-id any

bgp client-to-client reflection intra-cluster cluster-id 1.1.1.1

Cluster ID 1.1.1.1 has intracluster route reflection disabled (even though the second command is positive), because the first command is used to evaluate the update. The first command was negative, and once any level of configuration disables client-to-client reflection, no further evaluation is performed.

Another way to look at this example is that the second command, because it is in a positive form, defaults to the behavior of the first command (which is less specific). Thus, the second command is unnecessary.

Note that the second command would not appear in a configuration file because it is not a negative command.

Examples

In the following example, intracluster client-to-client reflection is enabled within any cluster:

```
Device(config)# router bgp 50000
Device(config-router)# bgp client-to-client reflection intra-cluster cluster-id any
```

In the following example, intracluster client-to-client reflection is enabled within the cluster that has cluster ID 10.1.4.5:

```
Device(config)# router bgp 50000
Device(config-router)# bgp client-to-client reflection intra-cluster cluster-id 10.1.4.5
```

In the following example, intracluster client-to-client reflection is disabled for any cluster:

```
Device(config)# router bgp 50000
Device(config-router)# no bgp client-to-client reflection intra-cluster cluster-id any
```

In the following example, intracluster client-to-client reflection is disabled within the cluster that has cluster ID 10.1.4.5:

```
Device(config)# router bgp 50000
Device(config-router)# no bgp client-to-client reflection intra-cluster cluster-id 10.1.4.5
```

Related Commands

Command	Description
bgp client-to-client reflection	Enables or restores route reflection from a BGP route reflector to clients.
bgp cluster-id	Sets the cluster ID on a route reflector in a route reflector cluster.
neighbor cluster-id	Configures the cluster ID per neighbor.
neighbor route-reflector-client	Configures the router as a BGP route reflector and configures the specified neighbor as its client.
show ip bgp cluster-ids	Displays cluster IDs, how many neighbors are in each cluster, and whether client-to-client route reflection is disabled for each cluster.

bgp cluster-id

To set the cluster ID on a route reflector in a route reflector cluster, use the **bgp cluster-id** command in router configuration mode. To remove the cluster ID, use the **no** form of this command.

bgp cluster-id *cluster-id*
no bgp cluster-id *cluster-id*

Syntax Description

cluster-id	Cluster ID of this router acting as a route reflector; maximum of 4 bytes. The ID can be specified in dotted or decimal format.

Command Default

The local router ID of the route reflector is used as the cluster ID when no ID is specified or when the **no** form of this command is entered.

Command Modes

Router configuration (config-router)

Command History

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

Usage Guidelines

Together, a route reflector and its clients form a *cluster* . When a single route reflector is deployed in a cluster, the cluster is identified by the router ID of the route reflector.

The **bgp cluster-id** command is used to assign a cluster ID to a route reflector when the cluster has one or more route reflectors. Multiple route reflectors are deployed in a cluster to increase redundancy and avoid a single point of failure. When multiple route reflectors are configured in a cluster, the same cluster ID is assigned to all route reflectors. This allows all route reflectors in the cluster to recognize updates from peers in the same cluster and reduces the number of updates that need to be stored in BGP routing tables.

Note All route reflectors must maintain stable sessions between all peers in the cluster. If stable sessions cannot be maintained, then overlay route reflector clusters should be used instead (route reflectors with different cluster IDs).

Examples

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

```
Router(config)# router bgp 50000

Router(config-router)# neighbor 192.168.70.24 route-reflector-client

Router(config-router)# bgp cluster-id 10.0.1.2
```

Related Commands

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

bgp confederation identifier

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

bgp confederation identifier *autonomous-system-number*
no bgp confederation identifier *autonomous-system-number*

Syntax Description

autonomous-system-number	Number of an autonomous system number used to configure a single autonomous system number to identify a group of smaller autonomous systems as a single confederation. 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.

Command Default

No BGP confederation identifier is identified.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
10.3	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.

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

Usage Guidelines

The **bgp confederation identifier** command is used to configure a single autonomous system number to identify a group of smaller autonomous systems as a single confederation.

A confederation can be used to reduce the internal BGP (iBGP) mesh by dividing a large single autonomous system into multiple subautonomous systems and then grouping them into a single confederation. The subautonomous systems within the confederation exchange routing information like iBGP peers. External peers interact with the confederation as if it were a single autonomous system.

Each subautonomous system is fully meshed within itself and has a few connections to other autonomous systems within the confederation. Next hop, Multi Exit Discriminator (MED), and local preference information is preserved throughout the confederation, allowing you to retain a single Interior Gateway Protocol (IGP) for all the autonomous systems.

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

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

If one member of a BGP confederation is identified using a 4-byte autonomous system number, all other members of a BGP confederation must be upgraded to support 4-byte autonomous system numbers.

Examples

In the following example, the routing domain is divided into autonomous systems 50001, 50002, 50003, 50004, 50005, and 50006 and is identified by the confederation identifier 50007. Neighbor 10.2.3.4 is a peer inside of the routing domain confederation. Neighbor 10.4.5.6 is a peer outside of the routing domain confederation. To external peers and routing domains, the confederation appears as a single autonomous system with the number 50007.

```
router bgp 50000
 bgp confederation identifier 50007
 bgp confederation peers 50001 50002 50003 50004 50005 50006
 neighbor 10.2.3.4 remote-as 50001
 neighbor 10.4.5.6 remote-as 40000
 end
```

In the following example, the routing domain is divided into autonomous systems using 4-byte autonomous system numbers 65538, 65536, and 65550 in asplain format and identified by the confederation identifier 65545. Neighbor 192.168.1.2 is a peer inside of the routing domain confederation. Neighbor 192.168.2.2 is a peer outside of the routing domain confederation. To external peers and routing domains, the confederation appears as a single autonomous system with the number 65545. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, or a later release.

```
router bgp 65550
 bgp confederation identifier 65545
 bgp confederation peers 65538 65536 65550
 neighbor 192.168.1.2 remote-as 65536
 neighbor 192.168.2.2 remote-as 65547
 end
```

In the following example, the routing domain is divided into autonomous systems using 4-byte autonomous system numbers 1.2 and 1.0 in asdot format and is identified by the confederation identifier 1.9. Neighbor 192.168.1.2 is a peer inside of the routing domain confederation. Neighbor 192.168.2.2 is a peer outside of the routing domain confederation. To external peers and routing domains, the confederation appears as a single autonomous system with the number 1.9. This example requires Cisco IOS Release 12.0(32)S12, 12.4(24)T, or Cisco IOS XE Release 2.3 where asdot notation is the only format for 4-byte autonomous system numbers. This configuration can also be performed using Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, or later releases.

```
router bgp 1.14
 bgp confederation identifier 1.9
 bgp confederation peers 1.2 1.0
 neighbor 192.168.1.2 remote-as 1.0
 neighbor 192.168.2.2 remote-as 1.11
 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.
bgp confederation peers	Configures subautonomous systems to belong to a single confederation.
router bgp	Configures the BGP routing process.

bgp confederation peers

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

bgp confederation peers *autonomous-system-number* [**...** *autonomous-system-number*]
no bgp confederation peers *autonomous-system-number* [**...** *autonomous-system-number*]

Syntax Description

autonomous-system-number	Autonomous system numbers for BGP peers that will belong to the confederation. Number in the range from 1 to 65535. The autonomous system number of the local router is not allowed to be specified in this command. • In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, 4-byte autonomous system numbers are supported in the range from 65536 to 4294967295 in asplain notation and in the range from 1.0 to 65535.65535 in asdot notation. • In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, 4-byte autonomous system numbers are supported in the range from 1.0 to 65535.65535 in asdot notation only. For more details about autonomous system number formats, see the **router bgp** command.

Command Default

No BGP peers are configured to be members of a BGP confederation.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
10.3	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.

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

Usage Guidelines

The **bgp confederation peers** command is used to configure multiple autonomous systems as a single confederation. The ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *autonomous-system-number* argument.

The autonomous system number of the router on which this command is being specified is not allowed in this command (not allowed as a confederation peer). If you specify the local router's autonomous system number in the **bgp confederation peers** command, the error message "Local member-AS not allowed in confed peer list" will appear.

The autonomous systems specified in this command are visible internally to the confederation. Each autonomous system is fully meshed within itself. Use the **bgp confederation identifier** command to specify the confederation to which the autonomous systems belong.

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

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

If one member of a BGP confederation is identified using a 4-byte autonomous system number, all other members of a BGP confederation must be upgraded to support 4-byte autonomous system numbers.

Examples

In the following example, autonomous systems 50001, 50002, 50003, 50004, and 50005 are configured to belong to a single confederation under the identifier 50000:

```
router bgp 50000
 bgp confederation identifier 50000
 bgp confederation peers 50001 50002 50003 50004 50005
```

In the following example, the routing domain is divided into autonomous systems using 4-byte autonomous system numbers 65538 and 65536, and is identified by the confederation identifier 65545. Neighbor 192.168.1.2 is a peer inside of the routing domain confederation. Neighbor 192.168.2.2 is a peer outside of the routing domain confederation. To external peers and routing domains, the confederation appears as a single autonomous system with the number 65545. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, or a later release.

```
router bgp 65550
 bgp confederation identifier 65545
 bgp confederation peers 65538 65536
 neighbor 192.168.1.2 remote-as 65536
 neighbor 192.168.2.2 remote-as 65547
 end
```

In the following example, the routing domain is divided into autonomous systems using 4-byte autonomous system numbers 1.2, 1.0, and 1.14 and is identified by the confederation identifier 1.9. Neighbor 192.168.1.2 is a peer inside of the routing domain confederation. Neighbor 192.168.2.2 is a peer outside of the routing domain confederation. To external peers and routing domains, the confederation appears as a single autonomous system with the number 1.9. This example requires Cisco IOS Release 12.0(32)S12, 12.4(24)T, or Cisco IOS XE Release 2.3 where asdot notation is the only format for 4-byte autonomous system numbers. This configuration can also be performed using Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, or later releases.

```
router bgp 1.14
 bgp confederation identifier 1.9
 bgp confederation peers 1.2 1.0 1.14
 neighbor 192.168.1.2 remote-as 1.0
 neighbor 192.168.2.2 remote-as 1.11
 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.
bgp confederation identifier	Specifies a BGP confederation identifier.
router bgp	Configures the BGP routing process.

bgp consistency-checker

To enable the BGP Consistency Checker feature, use the **bgp consistency-checker** command in router configuration mode. To disable the BGP Consistency Checker feature, use the **no** form of this command.

bgp consistency-checker {**error-message** | **auto-repair**} [**interval** *minutes*]
no bgp consistency-checker

Syntax Description

error-message	Specifies that when an inconsistency is found, the system will only generate a syslog message.
auto-repair	Specifies that when an inconsistency is found, the system will generate a syslog message and take action based on the type of inconsistency found.
interval *minutes*	(Optional) Specifies the interval at which the BGP consistency checker process occurs. • The range is 5 to 1440 minutes. The default is 1440 minutes (one day).

Command Default

No BGP consistency check is performed.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
15.1(2)S	This command was introduced.
Cisco IOS XE 3.3S	This command was integrated into Cisco IOS XE 3.3S.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

A BGP route inconsistency with a peer occurs when an update or a withdraw is not sent to a peer, and a routing absence can result. The BGP consistency checker feature is a low-priority process created to address this issue. This feature performs nexthop-label, RIB-out, and aggregation consistency checks. When BGP consistency checker is enabled, it is performed for all address families. Once the process identifies such an inconsistency:

- If the **error-message** keyword is specified, the system will report the inconsistency with a syslog message, and will also perform forceful aggregation reevaluation in the case of an aggregation inconsistency.
- If the **auto-repair** keyword is specified, the system will report the inconsistency with a syslog message and also take appropriate action, such as a route refresh request or an aggregation reevaluation, depending on the type of inconsistency.

Examples

In the following example, BGP consistency checker is enabled. If a BGP route inconsistency is found, the system will send a syslog message and take appropriate action.

```
Router(config)# router bgp 65000
Router(config-router)# bgp consistency-checker auto-repair
```

Related Commands

Command	Description
show ip bgp vpnv4 all inconsistency nexthop-label	Displays routes that have nexthop-label inconsistency found by BGP consistency checker.

bgp dampening

To enable BGP route dampening or change BGP route dampening parameters, use the **bgp dampening** command in address family or router configuration mode. To disable BGP dampening, use the **no** form of this command.

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

Syntax Description

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

Command Default

BGP dampening is disabled by default. The following values are used when this command is enabled without configuring any optional arguments:

half-life : 15 minutes *reuse*: 750 *suppress*: 2000 *max-suppress-time*: 4 times *half-life*

Command Modes

Address family configuration (config-router-af)

Router configuration (config-router)

Command History

Release	Modification
11.0	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.

Release	Modification
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 **bgp dampening** command is used to enable BGP route dampening. This command can be entered without any arguments or keywords. The *half-life*, *reuse*, *suppress*, and *max-suppress-time* arguments are position-dependent; meaning that if any of these arguments are entered, then all optional arguments must be entered.

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

Note This command is not supported in the address family configuration mode in Cisco IOS Release 12.2SX and later releases.

Examples

In the following example, the BGP dampening values are set to 30 minutes for the half life, 1500 for the reuse value, 10000 for the suppress value, and 120 minutes for the maximum suppress time:

```
Router(config)# router bgp 5
Router(config-router)# address-family ipv4 unicast

Router(config-router-af)# bgp dampening 30 1500 10000 120
Router(config-router-af)# end
```

In the following example, BGP dampening is applied to prefixes filtered through the route-map named BLUE:

```
Router(config)# ip prefix-list RED permit 10.0.0.0/8
Router(config)# !
Router(config)# route-map BLUE

Router(config-route-map)# match ip address ip prefix-list RED
Router(config-route-map)# exit
Router(config)# router bgp 50000

Router(config-router)# address-family ipv4
Router(config-router-af)# bgp dampening route-map BLUE
Router(config-router-af)# end
```

Related Commands

Command	Description
clear bgp nsap flap-statistics	Clears BGP flap statistics.
clear ip bgp dampening	Clears BGP route dampening information and unsuppresses the suppressed routes.
set dampening	Applies BGP dampening to prefixes filtered through a route map.

Command	Description
show ip bgp dampened-paths	Displays BGP dampened routes.
show ip bgp flap-statistics	Displays BGP flap statistics.

bgp default ipv4-unicast

To set the IP version 4 (IPv4) unicast address family as default for BGP peering session establishment, use the **bgp default ipv4-unicast** command in router configuration mode. To disable default IPv4 unicast address family for peering session establishment, use the **no** form of this command.

bgp default ipv4-unicast
no bgp default ipv4-unicast

Syntax Description

This command has no arguments or keywords.

Command Default

IPv4 address family routing information is advertised by default for each BGP routing session configured with the **neighbor remote-as** command, unless you first configure the **no bgp default ipv4-unicast** command before configuring the **neighbor remote-as** command.

Command Modes

Router configuration (config-router)

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 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.
15.2(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

The **bgp default ipv4-unicast** command is used to enable the automatic exchange of IPv4 address family prefixes. The **neighbor activate** address family configuration command must be entered in each IPv4 address family session before prefix exchange will occur.

Examples

In the following example, the automatic exchange of IP version 4 unicast address family routing information is disabled:

```
Device(config)# router bgp 50000
Device(config-router)# no bgp default ipv4-unicast
```

Related Commands

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

bgp default local-preference

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

bgp default local-preference *number*
no bgp default local-preference *number*

Syntax Description

number	Local preference value from 0 to 4294967295.

Command Default

Cisco IOS software applies a local preference value of 100 if this command is not enabled or if the **no** form of this command is entered.

Command Modes

Router configuration (config-router)

Command History

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

Usage Guidelines

The local preference attribute is a discretionary attribute that is used to apply the degree of preference to a route during the BGP best path selection process. This attribute is exchanged only between iBGP peers and is used to determine local policy. The route with the highest local preference is preferred.

Examples

In the following example, the local preference value is set to 200:

```
Router(config)# router bgp 50000

Router(config-router)# bgp default local-preference 200
```

Related Commands

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

bgp deterministic-med

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

bgp deterministic-med
no bgp deterministic-med

Syntax Description

This command has no arguments or keywords.

Command Default

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

Command Modes

Router configuration (config-router)

Command History

Release	Modification
11.1	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

In the following example, BGP is configured to compare the MED during path selection for routes advertised by the same subautonomous system within a confederation:

```
Router(config)# router bgp 50000
Router(config-router)# bgp deterministic-med
```

The following example **show ip bgp** command output shows how route selection is affected by the configuration of the **bgp deterministic-med** command. The order in which routes are received affects how routes are selected for best path selection when the **bgp deterministic-med** command is not enabled. The following sample output from the **show ip bgp** command shows three paths that are received for the same prefix (10.100.0.0), and the **bgp deterministic-med** command is not enabled:

```
Router# show ip bgp 10.100.0.0

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

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

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

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

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

```
Router# show ip bgp 10.100.0.0

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

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

```
Router# show ip bgp 10.100.0.0

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

Related Commands

Command	Description
bgp always-compare-med	Enables the comparison of the MED for paths from neighbors in different autonomous systems.
clear ip bgp	Resets a BGP connection or session.
show ip bgp	Displays entries in the BGP routing table.
show ip bgp neighbors	Displays information about the TCP and BGP connections to neighbors.

bgp dmzlink-bw

To configure BGP to distribute traffic proportionally over external links with unequal bandwidth when multipath load balancing is enabled, use the **bgp dmzlink-bw** command in address family configuration mode. To disable traffic distribution that is proportional to the link bandwidth, use the **no** form of this command.

bgp dmzlink-bw
no bgp dmzlink-bw

Syntax Description

This command has no arguments or keywords.

Command Default

BGP traffic is not distributed proportionally over external links with unequal bandwidth.

Command Modes

Address family configuration (config-router-af)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.0(24)S	This command was integrated into Cisco IOS Release 12.0(24)S.
12.2SX	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 **bgp dmzlink-bw** command is used to configure BGP to distribute traffic proportionally to the bandwidth of external links. This command is configured for multipath load balancing between directly connected external BGP (eBGP) neighbors. This command is used with BGP multipath features to configure load balancing over links with unequal bandwidth. The **neighbor dmzlink-bw** command must also be configured for each external link through which multipath load balancing is configured to advertise the link bandwidth as an extended community. The **neighbor send-community** command must be configured to exchange the link bandwidth extended community with internal BGP (iBGP) peers.

Examples

The following example shows how to configure the **bgp dmzlink-bw** command to allow multipath load balancing to distribute link traffic proportionally to the bandwidth of each external link and to advertise the bandwidth of these links to iBGP peers as an extended community:

```
Router(config)# router bgp 45000

Router(config-router)# neighbor 10.10.10.1 remote-as 100

Router(config-router)# neighbor 10.10.10.1 update-source Loopback 0

Router(config-router)# neighbor 10.10.10.3 remote-as 100

Router(config-router)# neighbor 10.10.10.3 update-source Loopback 0
Router(config-router)# neighbor 172.16.1.1 remote-as 200

Router(config-router)# neighbor 172.16.1.1 ebgp-multihop 1
```

```
Router(config-router)# neighbor 172.16.2.2 remote-as 200

Router(config-router)# neighbor 172.16.2.2 ebgp-multihop 1

Router(config-router)# address-family ipv4
Router(config-router-af)# bgp dmzlink-bw

Router(config-router-af)# neighbor 10.10.10.1 activate
Router(config-router-af)# neighbor 10.10.10.1 next-hop-self

Router(config-router-af)# neighbor 10.10.10.1 send-community both

Router(config-router-af)# neighbor 10.10.10.3 activate

Router(config-router-af)# neighbor 10.10.10.3 next-hop-self

Router(config-router-af)# neighbor 10.10.10.3 send-community both

Router(config-router-af)# neighbor 172.16.1.1 activate
Router(config-router-af)# neighbor 172.16.1.1 dmzlink-bw

Router(config-router-af)# neighbor 172.16.2.2 activate

Router(config-router-af)# neighbor 172.16.2.2 dmzlink-bw
Router(config-router-af)# maximum-paths ibgp 6
Router(config-router-af)# maximum-paths 6
```

Related Commands

Command	Description
neighbor dmzlink-bw	Configures BGP to advertise the bandwidth of links that are used to exit an autonomous system.
neighbor send-community	Specifies that a communities attribute should be sent to a BGP neighbor.

bgp enforce-first-as

To configure a router to deny an update received from an external BGP (eBGP) peer that does not list its autonomous system number at the beginning of the AS_PATH in the incoming update, use the **bgp enforce-first-as** command in router configuration mode. To disable this behavior, use the **no** form of this command.

bgp enforce-first-as
no bgp enforce-first-as

Syntax Description

This command has no arguments or keywords.

Command Default

The behavior of this command is enabled by default.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
12.0(3)S	This command was introduced.
12.0(26)S	The default behavior for this command was changed to enabled in Cisco IOS Release 12.0(26)S.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.3(2)	This command was integrated into Cisco IOS Release 12.3(2).
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
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 **bgp enforce-first-as** command is used to deny incoming updates received from eBGP peers that do not list their autonomous system number as the first segment in the AS_PATH attribute. Enabling this command prevents a misconfigured or unauthorized peer from misdirecting traffic (spoofing the local router) by advertising a route as if it was sourced from another autonomous system.

Examples

In the following example, all incoming updates from eBGP peers are examined to ensure that the first autonomous system number in the AS_PATH is the local AS number of the transmitting peer. In the follow example, updates from the 10.100.0.1 peer will be discarded if the first AS number is not 65001.

```
Router(config)# router bgp 50000

Router(config-router)# bgp enforce-first-as

Router(config-router)# address-family ipv4

Router(config-router-af)# neighbor 10.100.0.1 remote-as 65001
Router(config-router-af)# end
```

bgp enhanced-error

To restore the default behavior so that any malformed Update message is treat-as-withdraw, use the **bgp enhanced-error** command in router configuration mode. To disable the function, use the **no** form of this command.

bgp enhanced-error
no bgp enhanced-error

Syntax Description

This command has no arguments or keywords.

Command Default

The Enhanced Attribute Error Handling feature is enabled by default.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
15.2(4)S	This command was introduced.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS Release XE 3.7S.
15.3(1)T	This command was integrated into Cisco IOS Release 15.3(1)T.

Usage Guidelines

This command controls the BGP Enhanced Attribute Error Handling feature, which is enabled by default. This feature avoids peer sessions flapping due to malformed Update messages. Such Update messages are treat-as-withdraw.

This feature causes BGP to format the MP_REACH attribute in front of other attributes in the Update message. That is necessary because if any of the attribute lengths are malformed, there is no way of reaching the MP_REACH attribute if it is put at the end, and therefore no way to withdraw the prefixes. If the feature is disabled, BGP will format the MP_REACH attribute at the end of the Update message.

Examples

In the following example, Enhanced Attribute Error Handling is enabled (after it had been disabled):

```
router bgp 65000
 bgp enhanced-error
```

Related Commands

Command	Description
show ip bgp neighbors	Displays the configured discard and treat-as-withdraw attribute values and counters of incoming Update messages containing those attributes.

bgp fast-external-fallover

To configure a Border Gateway Protocol (BGP) routing process to immediately reset external BGP peering sessions if the link used to reach these peers goes down, use the **bgp fast-external-fallover c**ommand in router configuration mode. To disable BGP fast external fallover, use the **no** form of this command.

bgp fast-external-fallover
no bgp fast-external-fallover

Syntax Description

This command has no arguments or keywords.

Command Default

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

Command Modes

Router configuration (config-router)

Command History

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

Usage Guidelines

The **bgp fast-external-fallover** command is used to disable or enable fast external fallover for BGP peering sessions with directly connected external peers. The session is immediately reset if link goes down. Only directly connected peering sessions are supported.

If BGP fast external fallover is disabled, the BGP routing process will wait until the default hold timer expires (3 keepalives) to reset the peering session. BGP fast external fallover can also be configured on a per-interface basis using the **ip bgp fast-external-fallover** interface configuration command.

Examples

In the following example, the BGP fast external fallover feature is disabled. If the link through which this session is carried flaps, the connection will not be reset.

```
Router(config)# router bgp 50000

Router(config-router)# no bgp fast-external-fallover
```

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.
ip bgp fast-external-fallover	Configures per-interface BGP fast external fallover.

bgp graceful-restart

To enable the Border Gateway Protocol (BGP) graceful restart capability globally for all BGP neighbors, use the **bgp graceful-restart** command in address family or in router configuration mode. To disable the BGP graceful restart capability globally for all BGP neighbors, use the **no** form of this command.

bgp graceful-restart [{**extended** | **restart-time** *seconds* | **stalepath-time** *seconds*}] [**all**]
no bgp graceful-restart

Syntax Description

extended	(Optional) Enables BGP graceful restart extension.
restart-time *seconds*	(Optional) Sets the maximum time period that the local router will wait for a graceful-restart-capable neighbor to return to normal operation after a restart event occurs. The default value for this argument is 120 seconds. The configurable range of values is from 1 to 3600 seconds.
stalepath-time *seconds*	(Optional) Sets the maximum time period that the local router will hold stale paths for a restarting peer. All stale paths are deleted after this timer expires. The default value for this argument is 360 seconds. The configurable range of values is from 1 to 3600 seconds
all	(Optional) Enables BGP graceful restart capability for all address family modes.

Command Default

The following default values are used when this command is entered without any keywords or arguments:

restart-time : 120 seconds **stalepath-time**: 360 seconds

Note Changing the restart and stalepath timer values is not required to enable the BGP graceful restart capability. The default values are optimal for most network deployments, and these values should be adjusted only by an experienced network operator.

Command Modes

Address-family configuration (config-router-af)

Router configuration (config-router)

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(28)SB	Support for this command was added into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	Support for IPv6 was added. The optional **all** keyword was added.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE .
Cisco IOS XE Release 3.11S	This command was modified. The **extended** keyword was added.

Usage Guidelines

The **bgp graceful-restart** command is used to enable or disable the graceful restart capability globally for all BGP neighbors in a BGP network. 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 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.

The BGP graceful restart capability is enabled by default when a supporting version of Cisco IOS software is installed. The default timer values for this feature are optimal for most network deployments. We recommend that they are adjusted only by experienced network operators. When adjusting the timer values, the restart timer should not be set to a value greater than the hold time that is carried in the OPEN message. If consecutive restart operations occur, routes (from a restarting router) that were previously marked as stale will be deleted.

Note Changing the restart and stalepath timer values is not required to enable the BGP graceful restart capability. The default values are optimal for most network deployments, and these values should be adjusted only by an experienced network operator.

Examples

In the following example, the BGP graceful restart capability is enabled:

```
Router# configure terminal
Router(config)# router bgp 65000
Router(config-router)# bgp graceful-restart
```

In the following example, the restart timer is set to 130 seconds:

```
Router# configure terminal
Router(config)# router bgp 65000
Router(config-router)# bgp graceful-restart restart-time 130
```

In the following example, the stalepath timer is set to 350 seconds:

```
Router# configure terminal
Router(config)# router bgp 65000
Router(config-router)# bgp graceful-restart stalepath-time 350
```

In the following example, the **extended** keyword is used:

```
Router# configure terminal
Router(config)# router bgp 65000
Router(config-router)# bgp graceful-restart extended
```

Related Commands

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

bgp graceful-shutdown all

To enable the Border Gateway Protocol (BGP) graceful shutdown capability globally for all BGP neighbors, including virtual routing and forwarding (VRF) neighbors, use the **bgp graceful-shutdown all** command in router configuration mode. To disable the BGP graceful shutdown capability, use the **no** form of this command.

bgp graceful-shutdown all {**neighbors** | **vrfs**} {*shutdown-time* {**community** {*community-number formatted-community-value*} [**local-preference** [*local-pref-value*]] | **local-preference** *local-pref-value* [**community** [{*community-number formatted-community-value*}]]} | **activate**}

no bgp graceful-shutdown all {**neighbors** | **vrfs**} {*shutdown-time* {**community** {*community-number formatted-community-value*} [**local-preference** [*local-pref-value*]] | **local-preference** *local-pref-value* [**community** [{*community-number formatted-community-value*}]]} | **activate**}

Syntax Description

neighbors	Enables graceful shutdown of all BGP neighbors.
vrfs	Enables graceful shutdown of BGP sessions associated only with VRF neighbors.
shutdown-time	Sets the shutdown time for all BGP neighbors or only for VRF neighbors. The shutdown time ranges from 30 to 65535 seconds.
community	Sets community for all BGP graceful shutdown routes.
community-number	Sets the community value for BGP graceful shutdown routes. This value ranges from 1 to 4294967295.
formatted-community-value	Sets the community value for BGP graceful shutdown routes in the aa:nn format.
local-preference	Sets local preference for all BGP graceful shutdown routes.
local-pref-value	Sets local preference value for all BGP graceful shutdown routes. This value ranges from 1 to 4294967295.
activate	Enables activation of graceful shutdown of all BGP neighbors or only VRF neighbors.

Command Default

The BGP graceful-shutdown feature is disabled by default.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Release 3.11S	This command was introduced.

Usage Guidelines

Using the BGP GSHUT enhancement feature, you can gracefully shutdown either all (including VRF) neighbors or only the VRF neighbors that are already configured across all BGP sessions. To enable the BGP GSHUT enhancement feature on the device, you must configure either the **community** keyword or the **local-preference** keyword in the **bgp graceful-shutdown all** command. Use the **activate** keyword to activate graceful shutdown either across all neighbors or only across all VRF neighbors, across all BGP sessions.

Example

The following example shows how to enable and activate the BGP GSHUT enhancement feature across all neighbors:

```
Device> enable
Device# configure terminal
Device(config)# router bgp 65000
Device(config-router)# bgp graceful-shutdown all neighbors 180 local-preference 20 community
 10
Device(config-router)# bgp graceful-shutdown all neighbors activate
Device(config-router)# end
```

Note In this example, the neighbors will gracefully shutdown within the specified duration of 180 seconds.

Following is sample output from the **show ip bgp** command, which displays the graceful shutdown time for each neighbor:

Note In this example, there are two IPv4 neighbors configured with IP address 10.2.2.2 and 172.16.2.1 and one VRF neighbor, tagged v1, is configured with IP address 192.168.1.1.

```
Device# show ip bgp neighbors 10.2.2.2 | include shutdown

Graceful Shutdown Timer running, schedule to reset the peer in 00:02:47 seconds
Graceful Shutdown Localpref set to 20
Graceful Shutdown Community set to 10

Device# show ip bgp neighbors 172.16.2.1 | include shutdown

Graceful Shutdown Timer running, schedule to reset the peer in 00:02:38 seconds
Graceful Shutdown Localpref set to 20
Graceful Shutdown Community set to 10

Device# show ip bgp vpnv4 vrf v1 neighbors 192.168.1.1 | include shutdown

Graceful Shutdown Timer running, schedule to reset the peer in 00:01:45 seconds
Graceful Shutdown Localpref set to 20
Graceful Shutdown Community set to 10
```

Following is sample output from the **show running-config** command, which displays information associated with the BGP session in router configuration mode:

```
Device# show running-config | session router bgp

router bgp 65000
bgp log-neighbor-changes
bgp graceful-shutdown all neighbors 180 local-preference 20 community 10
network 10.1.1.0 mask 255.255.255.0
neighbor 10.2.2.2 remote-as 40
neighbor 10.2.2.2 shutdown
neighbor 172.16.2.1 remote-as 10
neighbor 172.16.2.1 shutdown
!
```

```
address-family vpnv4
neighbor 172.16.2.1 activate
neighbor 172.16.2.1 send-community both
exit-address-family
!
address-family ipv4 vrf v1
neighbor 192.168.1.1 remote-as 30
neighbor 192.168.1.1 shutdown
neighbor 192.168.1.1 activate
neighbor 192.168.1.1 send-community both
exit-address-family
```

Related Commands

Command	Description
show ip bgp	Displays entries in the BGP routing table.
show running-config	Displays running configuration on a device.

bgp inject-map

To configure conditional route injection to inject more specific routes into a Border Gateway Protocol (BGP) routing table, use the **bgp inject-map** command in address family or router configuration mode. To disable a conditional route injection configuration, use the **no** form of this command.

bgp inject-map *inject-map* **exist-map** *exist-map* [**copy-attributes**]
no bgp inject-map *inject-map* **exist-map** *exist-map*

Syntax Description

inject-map	Name of the route map that specifies the prefixes to inject into the local BGP routing table.
exist-map *exist-map*	Specifies the name of the route map containing the prefixes that the BGP speaker will track.
copy-attributes	(Optional) Configures the injected route to inherit attributes of the aggregate route.

Command Default

No specific routes are injected into a BGP routing table.

Command Modes

Address family configuration (config-router-af)

Router configuration (config-router)

Command History

Release	Modification
12.0(14)ST	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX.

Usage Guidelines

The **bgp inject-map** command is used to configure conditional route injection. Conditional route injection allows you to originate a more specific prefix into a BGP routing table without a corresponding match. Two route maps (*exist-map*and *inject-map*) are configured in global configuration mode and then specified with the **bgp inject-map** command in address family or router configuration mode.

The *exist-map* argument specifies a route map that defines the prefix that the BGP speaker will track. This route map must contain a **match ip address prefix-list** command statement to specify the aggregate prefix and a **match ip route-source prefix-list** command statement to specify the route source.

The *inject-map* argument defines the prefixes that will be created and installed into the routing table. Injected prefixes are installed in the local BGP RIB. A valid parent route must exist; Only prefixes that are equal to or more specific than the aggregate route (existing prefix) can be injected.

The optional **copy-attributes** keyword is used to optionally configure the injected prefix to inherit the same attributes as the aggregate route. If this keyword is not entered, the injected prefix will use the default attributes for locally originated routes.

Examples

In the following example, conditional route injection is configured. Injected prefixes will inherit the attributes of the aggregate (parent) route.

```
Router(config)# ip prefix-list ROUTE permit 10.1.1.0/24
Router(config)# ip prefix-list ROUTE_SOURCE permit 10.2.1.1/32
Router(config)# ip prefix-list ORIGINATED_ROUTES permit 10.1.1.0/25
Router(config)# ip prefix-list ORIGINATED_ROUTES permit 10.1.1.128/25
Router(config)# route-map LEARNED_PATH permit 10
Router(config-route-map)# match ip address prefix-list ROUTE
Router(config-route-map)# match ip route-source prefix-list ROUTE_SOURCE
Router(config-route-map)# exit
Router(config)# route-map ORIGINATE permit 10
Router(config-route-map)# set ip address prefix-list ORIGINATED_ROUTES
Router(config-route-map)# set community 14616:555 additive
Router(config-route-map)# exit
Router(config)# router bgp 50000
Router(config-router)# address-family ipv4
Router(config-router-af)# bgp inject-map ORIGINATE exist-map LEARNED_PATH copy-attributes
Router(config-router-af)# end
```

Related Commands

Command	Description
ip prefix-list	Creates an entry in a prefix list.
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 route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
set ip address prefix-list	Sets a route to criteria specified in the source prefix list.
set community	Sets the BGP communities attribute.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
show ip bgp	Displays entries in the BGP routing table.
show ip bgp injected-paths	Displays injected routes or prefixes in the BGP routing table.
show ip prefix-list	Displays information about a prefix list or prefix list entries.

bgp listen

To associate a subnet range with a Border Gateway Protocol (BGP) peer group and activate the BGP dynamic neighbors feature, use the **bgp listen** command in router configuration mode. To disable the BGP dynamic neighbors feature, use the **no** form of this command.

bgp listen [{ **block** *ip-address* **limit** *max-number* | **range** *network* / *length* **peer-group** *peer-group-name* **persistent** *minutes* / *disable* }]
no bgp listen [{ **block** *ip-address* **limit** *max-number* | **range** *network* / *length* **peer-group** *peer-group-name* **persistent** *minutes* / *disable* }]

Syntax Description

block	(Optional) Blocks a specific dynamic peering.
ip-address	Specifies the Dynamic peering address.
limit	(Optional) Sets a maximum limit number of BGP dynamic subnet range neighbors.
max-number	(Optional) Number from 1 to 5000. Default is 100.
range	(Optional) Specifies a subnet range that is to be associated with a specified peer group.
network / *length*	(Optional) The IP prefix representing a subnet, and the length of the subnet mask in bits. The *network* argument can be any valid IP prefix. The *length* argument can be a number from 0 to 32.
peer-group	(Optional) Specifies a BGP peer group that is to be associated with the specified subnet range.
peer-group-name	(Optional) Name of a BGP peer group. This peer group is referred to as a listen range group.
persistent	(Optional) Enables the persistent dynamic neighbors globally. The value ranges from 1 to 65535 minutes.
disable	Disables persistent neighbors for the listen range.

Command Default

No subnets are associated with a BGP listen range group, and the BGP dynamic neighbor feature is not activated.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
15.1(2)T	This command was integrated into Cisco IOS Release 15.1(2)T.
15.0(1)S	This command was integrated into Release 15.0(1)S.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS Release 3.1S.

Release	Modification
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
Cisco IOS XE 17.13.1a	This command was modified. The **persistent** keyword was added.

Usage Guidelines

Use the **limit** keyword and *max-number* argument to define the global maximum number of BGP dynamic neighbors that can be created.

BGP dynamic neighbors are configured using a range of IP addresses and BGP peer groups. Each range can be configured as a subnet IP address. After a subnet range is configured for a BGP peer group, and a TCP session is initiated for an IP address in the subnet range, a new BGP neighbor is dynamically created as a member of that group. The new BGP neighbor will inherit any configuration for the peer group. Only IPv4 peering is supported. The output for three **show** commands has been updated to display information about dynamic neighbors. The commands are **show ip bgp neighbors**, **show ip bgp peer-group**, and the **show ip bgp summary** command.

Use the **bgp listen range peer-group persistent** command to configure the Persistent Dynamic Neighbor feature on a specific peer group.

Examples

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

Router 1

```
enable
configure terminal
router bgp 45000
 bgp log-neighbor-changes
 neighbor group192 peer-group
 bgp listen range 192.168.0.0/16 peer-group group192
 neighbor group192 ebgp-multihop 255
 neighbor group192 remote-as 40000 alternate-as 50000
 address-family ipv4 unicast
 neighbor group192 activate
 end
```

Router 2

```
enable
configure terminal
router bgp 50000
 neighbor 192.168.3.1 remote-as 45000
 exit
If the show ip bgp summary
 command is now entered on Router 1, the output shows the dynamically created BGP neighbor,
 192.168.3.2.
Router1# show ip bgp summary
```

```
BGP router identifier 192.168.3.1, local AS number 45000
BGP table version is 1, main routing table version 1
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
*192.168.3.2    4 50000       2       2        0    0    0 00:00:37        0
* Dynamically created based on a listen range command
Dynamically created neighbors: 1/(100 max), Subnet ranges: 1
BGP peergroup group192 listen range group members:
  192.168.0.0/16
```

Related Commands

Command	Description
neighbor peer-group	Creates a BGP peer group.
neighbor remote-as	Adds an entry to the BGP or multiprotocol BGP neighbor table.
router bgp	Configures the BGP routing process.
show ip bgp summary	Displays the status of all BGP connections.

bgp log-neighbor-changes

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

bgp log-neighbor-changes
no bgp log-neighbor-changes

Syntax Description

This command has no arguments or keywords.

Command Default

Logging of BGP neighbor resets is not enabled.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
11.1CC	This command was introduced.
12.0	This command was integrated into Cisco IOS release 12.0.
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.
12.2(33)SRB	Support for IPv6 was added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

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

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

The neighbor status change messages are not tracked if the **bgp log-neighbor-changes** command is not enabled, except for the reset reason, which is always available as output of the **show ip bgp neighbors** and **show bgp ipv6 neighbors** commands.

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

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

Examples

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

```
Device(config)# bgp router 40000
Device(config-router)# bgp log-neighbor-changes
```

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.
eigrp log-neighbor-changes	Enables the logging of neighbor adjacency changes to monitor the stability of the routing system and to help detect problems.
logging buffered	Logs messages to an internal buffer.
show ip bgp ipv4	Displays information about the TCP and BGP connections to neighbors.
show ip bgp neighbors	Displays information about BGP neighbors.
show logging	Displays the state of logging (syslog).

bgp maxas-limit

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

bgp maxas-limit *number*
no bgp maxas-limit

Syntax Description

number	Maximum number of autonomous system numbers in the AS-path attribute of the BGP Update message, ranging from 1 to 254. In addition to setting the limit on the number of autonomous system numbers within the AS-path segment, the command limits the number of AS-path segments to ten. The behavior to allow ten AS-path segments is built into the **bgp maxas-limit** command. **Note** In some earlier Cisco IOS software releases, values up to 2000 can be configured. Cisco does not recommend that a value higher than 254 be configured. These releases also have no limit on the number of autonomous system segments in the AS-path attribute.

Command Default

No routes are discarded.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
12.2	This command was introduced.
12.0(17)S	This command was integrated into Cisco IOS Release 12.0(17)S.
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 **bgp maxas-limit** command is used to limit the number of autonomous system numbers in the AS-path attribute that are permitted in inbound routes. If a route is received with an AS-path segment that exceeds the configured limit, the BGP routing process will discard the route.

Examples

This example sets a maximum number of autonomous systems numbers in the AS-path attribute to 30:

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

Related Commands

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

bgp maxcommunity-limit

To configure Border Gateway Protocol (BGP) to allow routes that have several community attributes from any neighbor that exceed the specified value in the number of communities, use the **bgp maxcommunity-limit** command in router configuration mode. To return the device to default operation, use the **no** form of this command.

bgp maxcommunity-limit *number*
no bgp maxcommunity-limit

Syntax Description

number	Maximum number of communities in the community attribute. Range is from 1 to 1018.

Command Default

No routes are discarded.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE 3.7	This command was introduced.

Usage Guidelines

The **bgp maxcommunity-limit** command is used to limit the number of communities in a community attribute from any neighbor.

Examples

This example sets the maximum community number in a community attribute to 30:

```
Device(config)# router bgp 40000
Device(config-router)# bgp maxcommunity-limit 30
```

Related Commands

Command	Description
bgp maxextcommunity-limit	Limits the number of extended communities in an extended community attribute from any neighbor.

bgp maxextcommunity-limit

To configure Border Gateway Protocol (BGP) to allow routes that have several extended community attributes from any neighbor that exceed the specified value in the number of extended communities, use the **bgp maxextcommunity-limit** command in router configuration mode. To return the device to default operation, use the **no** form of this command.

bgp maxextcommunity-limit *number*
no bgp maxextcommunity-limit

Syntax Description

number	Maximum number of extended communities in an extended community attribute. Range is from 1 to 509.

Command Default

No routes are discarded.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE 3.7	This command was introduced.

Usage Guidelines

The **bgp maxextcommunity-limit** command is used to limit the number of extended communities in an extended community attribute from any neighbor.

Examples

This example sets the extended maximum community number in an extended community attribute to 30:

```
Device(config)# router bgp 40000
Device(config-router)# bgp maxextcommunity-limit 30
```

Related Commands

Command	Description
bgp maxcommunity-limit	Limits the number of communities in a community attribute from any neighbor.

bgp mpls-local-label

To enable Border Gateway Protocol (BGP) local label allocation for unadvertised /32 prefixes, use the **bgp mpls-local-label** command in address family configuration mode. To disable BGP local label allocation for unadvertised /32 prefixes, use the **no** form of this command.

bgp mpls-local-label
no bgp mpls-local-label

Syntax Description

This command has no arguments or keywords.

Command Default

BGP local label allocation for unadvertised /32 prefixes is not enabled.

Command Modes

Address-family configuration (config-router-af)

Command History

Release	Modification
15.2(4)S	This command was introduced.

Usage Guidelines

The **bgp mpls-local-label** command enables BGP local label allocation for unadvertised /32 prefixes. The local label allocation is done at the time of bestpath calculation for the route. The allocation is done for /32 prefixes learned from BGP peers with which the label capability was negotiated at the time of session establishment. Subsequently, if that prefix is chosen during update generation and for transmission to a certain update-group member, a new label will not be allocated for that route. The route will be advertised with the label allocated during bestpath computation in accordance with the peer's policies.

Turning on and off this command (toggling) will cause all existing sessions configured under IPv4 Address Family Identifiers (AFIs) to be flapped and all routes will be relearned for local label allocation during bestpath computation. A warning message also will be displayed to notify you that additional labels are required for /32 prefixes.

Note The **bgp mpls-local-label** command is supported only on the Cisco 7600 series router.

Examples

```
Device(config)# router bgp 100
Device(config-router)# address-family ipv4
Device(config-router-af)# bgp mpls-local-label
```

Related Commands

Command	Description
address-family ipv4	Enters address family configuration mode for configuring routing sessions, such as BGP, that use standard IPv4 address prefixes.
router bgp	Configures the BGP routing process.

bgp nexthop

To configure Border Gateway Protocol (BGP) next-hop address tracking, use the **bgp nexthop** command in address family or router configuration mode. To disable BGP next-hop address tracking, use the **no** form of this command.

bgp nexthop {**trigger** {**delay** *seconds* | **enable**} | **route-map** *map-name*}
no bgp nexthop {**trigger** {**delay** | **enable**} | **route-map** *map-name*}

Syntax Description

trigger	Specifies the use of BGP next-hop address tracking. Use this keyword with the **delay** keyword to change the next-hop tracking delay. Use this keyword with the **enable** keyword to enable next-hop address tracking.
delay	Changes the delay interval between checks on updated next-hop routes installed in the routing table.
seconds	Number of seconds specified for the delay. Range is from 0 to 100. Default is 5.
enable	Enables BGP next-hop address tracking.
route-map	Specifies the use of a route map that is applied to the route in the routing table that is assigned as the next-hop route for BGP prefixes.
map-name	Name of a route map.

Command Default

BGP next-hop address tracking is enabled by default for IPv4 and VPNv4 address families. It is also enabled by default for the VPNv6 address family as of Cisco IOS Release 12.2(33)SB6.

Command Modes

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

Command History

Release	Modification
12.0(29)S	This command was introduced.
12.0(31)S	The default delay interval was changed from 1 to 5 seconds.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.4(4)T	The **route-map** keyword and *map-name* argument were added to support the BGP Selective Address Tracking feature.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2(33)SRB	The **route-map** keyword and *map-name* argument were added to support the BGP Selective Address Tracking feature.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SB6	This command was modified. Next-hop address tracking is enabled by default for VPNv6 prefixes.
15.0(1)SY	This command was modified. Support for the **route-map**keyword and *map-name* argument was disabled in Cisco IOS Release 15.0(1)SY.

Usage Guidelines

BGP next-hop address tracking is event driven. BGP prefixes are automatically tracked as peering sessions are established. Next-hop changes are rapidly reported to BGP as they are updated in the routing information base (RIB). This optimization improves overall BGP convergence by reducing the response time to next-hop changes for routes installed in the RIB. When a best-path calculation is run in between BGP scanner cycles, only the changes are processed and tracked.

Note BGP next-hop address tracking improves BGP response time significantly. However, unstable Interior Gateway Protocol (IGP) peers can introduce instability to BGP. We recommend that you aggressively dampen unstable IGP peering sessions to mitigate the possible impact to BGP.

Note BGP next-hop address tracking is not supported under the IPv6 address family.

Use the **trigger**keyword with the **delay** keyword and *seconds* argument to change the delay interval between routing table walks for BGP next-hop address tracking. You can increase the performance of BGP next-hop address tracking by tuning the delay interval between full routing table walks to match the tuning parameters for the IGP. The default delay interval is 5 seconds, which is an optimal value for a fast-tuned IGP. In the case of an IGP that converges more slowly, you can change the delay interval to 20 seconds or more, depending on the IGP convergence time.

Use the **trigger**keyword with the **enable**keyword to enable BGP next-hop address tracking. BGP next-hop address tracking is enabled by default.

Use the **route-map** keyword and *map-name* argument to allow a route map to be used. The route map is used during the BGP best-path calculation and is applied to the route in the routing table that covers the Next_Hop attribute for BGP prefixes. If the next-hop route fails the route-map evaluation, the next-hop route is marked as unreachable. This command is per address family, so different route maps can be applied for next-hop routes in different address families.

Note The **route-map**keyword and *map-name*argument are not supported in Cisco IOS Release 15.0(1)SY.

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

Examples

The following example shows how to change the delay interval between routing table walks for BGP next-hop address tracking to occur every 20 seconds under an IPv4 address family session:

```
router bgp 50000
 address-family ipv4 unicast
 bgp nexthop trigger delay 20
 end
```

The following example shows how to disable next-hop address tracking for the IPv4 address family:

```
router bgp 50000
 address-family ipv4 unicast
 no bgp nexthop trigger enable
 end
```

The following example shows how to configure a route map that permits a route to be considered as a next-hop route only if the address mask length is more than 25. This configuration will avoid any prefix aggregates being considered as a next-hop route.

```
router bgp 45000
 address-family ipv4 unicast
 bgp nexthop route-map CHECK-NEXTHOP
 exit-address-family
 exit
ip prefix-list FILTER25 seq 5 permit 0.0.0.0/0 ge 25
route-map CHECK-NEXTHOP permit 10
 match ip address prefix-list FILTER25
 end
```

Related Commands

Command	Description
match ip address	Matches IP addresses defined by a prefix list.
match source-protocol	Matches the route type based on the source protocol.

bgp nexthop trigger delay

The **trigger** and **delay** keywords for the **bgp nexthop** command are no longer documented as a separate command.

The information for using the **trigger** and **delay** keywords for the **bgp nexthop** command has been incorporated into the **bgp nexthop** command documentation. See the **bgp nexthop** command documentation for more information.

bgp nexthop trigger enable

The **trigger** and **enable** keywords for the **bgp nexthop** command are no longer documented as a separate command.

The information for using the **trigger** and **enable** keywords for the **bgp nexthop** command has been incorporated into the **bgp nexthop** command documentation. See the **bgp nexthop** command documentation for more information.

bgp nopeerup-delay

To configure the time duration that Border Gateway Protocol (BGP) waits for the first peer to come up before populating the routing information base (RIB), use the **bgp nopeerup-delay** command in router configuration mode. To remove the configured values, use the **no** form of this command.

bgp nopeerup-delay {**cold-boot** | **nsf-switchover** | **post-boot** | **user-initiated**} *seconds*
no bgp nopeerup-delay {**cold-boot** | **nsf-switchover** | **post-boot** | **user-initiated**} *seconds*

Syntax Description

cold-boot	Specifies the delay time for the first peer to come up after a cold boot.
nsf-switchover	Specifies the delay time for the first peer to come up post Non-Stop Forwarding (NSF) switchover.
post-boot	Specifies the delay time for the first peer to come up once the system is booted and all peers go down.
user-initiated	Specifies the delay time for the first peer to come up after a manual clear of BGP peers by the administrative user.
seconds	Delay in seconds. Valid values are from 1 to 3600.

Command Default

Delay time is not configured.

Command Modes

Router configuration (config-router)

Command History

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

Usage Guidelines

In a Virtual Switching System (VSS), Open Shortest Path First (OSPF) NSF Engineering Task Force (IETF) operations and BGP are configured and peers are propagated through OSPF. In such a VSS, the OSPF restart interval should be shorter than the time BGP waits for the first peer to come up before populating the RIB; otherwise traffic will be dropped. To make the OSPF restart interval shorter than the time BGP waits for the first peer to come up, use the **nsf ietf restart-interval**command. To change the time duration that BGP waits for the first peer to come up, and make it longer than the OSPF restart interval, use the **bgp nopeerup-delay**command.

Examples

The following example shows how to configure the delay time to 234 seconds for the first peer to come up after NSF switchover.

```
Router(config)# router bgp 100
Router(config-router)# bgp nopeerup-delay nsf-switchover 234
```

Related Commands

Command	Description
clear ip bgp peer-group	Resets the BGP connections using hard or soft reconfiguration for all the members of a BGP peer group.
nsf ietf restart-interval	Enables IETF NSF operations on a router that is running OSPF.
router bgp	Configures the BGP routing process.

bgp recursion host

To enable the recursive-via-host flag for IP Version 4 (IPv4), VPN Version 4 (VPNv4), virtual routing and forwarding (VRF) address families, and IPv6 address families, use the **bgp recursion host** command in address family configuration or router configuration mode. To disable the recursive-via-host flag, use the **no** form of this command.

bgp recursion host
no bgp recursion host

Syntax Description

This command has no arguments or keywords.

Command Default

For an internal Border Gateway Protocol (iBGP) IPv4 address family, irrespective of whether Prefix Independent Convergence (PIC) is enabled, the recursive-via-host flag in Cisco Express Forwarding is not set.

For the VPNv4 and IPv4 VRF address families, the recursive-via-host flag is set and the **bgp recursion host** command is automatically restored when PIC is enabled under the following conditions:

- The **bgp additional-paths install** command is enabled.
- The **bgp advertise-best-external** command is enabled.

Command Modes

Address family configuration (config-router-af)

Router configuration (config-router)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.
Cisco IOS XE Release 3.3S	Support for IPv6 address family configuration mode was added.
15.1(2)S	Support for IPv6 address family configuration mode was added.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

The **bgp recursion host** command is used to help Cisco Express Forwarding during traffic route absence when a node failure occurs.

For link protection, BGP automatically restricts the recursion for the next hop resolution of connected routes. These routes are provided by the route reflector, which receives the prefix from another provider edge (PE) router that needs the customer edge (CE) router to be protected.

For node protection, BGP automatically restricts the recursion for the next hop resolution of host routes. These routes are provided by the route reflector, which receives the prefix from the host PE router. If a PE router or Autonomous System Boundary Router (ASBR) fails, for the **bgp recursion host** command to work, the PE routers must satisfy the following options:

- The host prefix must be used on the PE loopback interfaces.
- The next-hop-self must be configured on iBGP sessions.
- The **recursive via host prefix** command must be configured.

To enable Cisco Express Forwarding to use strict recursion rules for an IPv4 address family, you must configure the **bgp recursion host** command that enables the recursive-via-host flag when PIC is enabled.

The recursive-via-connected flag is set for directly connected peers only. For example, if the **bgp additional-paths install** command is configured in IPv4 and IPv4 VRF address family configuration modes, the running configuration shows the following details:

```
address-family ipv4
bgp additional-paths-install
no bgp recursion host
!
address-family ipv4 vrf red
bgp additional-paths-install
bgp recursion host
```

In the case of an external Border Gateway Protocol (eBGP) directly connected peers route exchange, the recursion is disabled for the connected routes. The recursive-via-connected flag is automatically set in the RIB and Cisco Express Forwarding for the routes from the eBGP single-hop peers.

For all the VPNs, irrespective of whether PIC is enabled, when the **bgp recursion host** command is configured in VPNv4 and IPv4 address family configuration modes, the normal recursion rules are disabled and only recursion via host-specific routes is allowed for primary, backup, and multipaths under those address families. To enable the normal recursion rules, configure the **no bgp recursion host** command in VPNv4 and IPv4 address family configuration modes.

Examples

The following example shows the configuration of the **bgp advertise-best-external** and **bgp recursion host** commands:

```
Router> enable
Router# configure terminal
Router(config)# router ospf 10
Router(config-router)# log-adjacency-changes
Router(config-router)# redistribute connected subnets
Router(config-router)# network 192.168.0.0 0.0.255.255 area 0
Router(config-router)# router bgp 64500
Router(config-router)# no synchronization
Router(config-router)# bgp log-neighbor-changes
Router(config-router)# neighbor 10.5.5.5 remote-as 64500
Router(config-router)# neighbor 10.5.5.5 update-source Loopback0
Router(config-router)# neighbor 10.6.6.6 remote-as 64500
Router(config-router)# neighbor 10.6.6.6 update-source Loopback0
Router(config-router)# no auto-summary
Router(config-router)# address-family vpnv4
Router(config-router-af)# neighbor 10.5.5.5 activate
Router(config-router-af)# neighbor 10.5.5.5 send-community extended
Router(config-router-af)# neighbor 10.6.6.6 activate
Router(config-router-af)# neighbor 10.6.6.6 send-community extended
```

```
Router(config-router-af)# exit-address-family
Router(config-router)# address-family ipv4 vrf test1
Router(config-router-af)# no synchronization
Router(config-router-af)# bgp advertise-best-external
Router(config-router-af)# bgp recursion host
Router(config-router-af)# neighbor 192.168.9.2 remote-as 64511
Router(config-router-af)# neighbor 192.168.9.2 fall-over bfd
Router(config-router-af)# neighbor 192.168.9.2 activate
Router(config-router-af)# neighbor 192.168.9.2 as-override
Router(config-router-af)# neighbor 192.168.9.2 route-map LOCAL_PREF in
Router(config-router-af)# exit-address-family
```

The following example shows the configuration of the **bgp additional-paths install** and **bgp recursion host** commands:

```
Router> enable
Router# configure terminal
Router(config)# router ospf 10
Router(config-router)# log-adjacency-changes
Router(config-router)# redistribute connected subnets
Router(config-router)# network 192.168.0.0 0.0.255.255 area 0
Router(config-router)# router bgp 64500
Router(config-router)# no synchronization
Router(config-router)# bgp log-neighbor-changes
Router(config-router)# neighbor 10.5.5.5 remote-as 64500
Router(config-router)# neighbor 10.5.5.5 update-source Loopback0
Router(config-router)# neighbor 10.6.6.6 remote-as 64500
Router(config-router)# neighbor 10.6.6.6 update-source Loopback0
Router(config-router)# no auto-summary
Router(config-router)# address-family vpnv4
Router(config-router-af)# neighbor 10.5.5.5 activate
Router(config-router-af)# neighbor 10.5.5.5 send-community extended
Router(config-router-af)# neighbor 10.6.6.6 activate
Router(config-router-af)# neighbor 10.6.6.6 send-community extended
Router(config-router-af)# exit-address-family
Router(config-router)# address-family ipv4 vrf test1
Router(config-router-af)# no synchronization
Router(config-router-af)# bgp additional-paths install
Router(config-router-af)# bgp recursion host
Router(config-router-af)# neighbor 192.168.9.2 remote-as 64511
Router(config-router-af)# neighbor 192.168.9.2 fall-over bfd
Router(config-router-af)# neighbor 192.168.9.2 activate
Router(config-router-af)# neighbor 192.168.9.2 as-override
Router(config-router-af)# neighbor 192.168.9.2 route-map LOCAL_PREF in
Router(config-router-af)# exit-address-family
```

The following example shows the best external routes and the BGP recursion flags enabled:

```
Router# show ip bgp vpnv4 vrf test1 192.168.13.1

BGP routing table entry for 400:1:192.168.13.0/24, version 4
Paths: (2 available, best #2, table test1)
  Advertise-best-external
  Advertised to update-groups:
     1
  64511, imported path from 300:1:192.168.13.0/24
    10.7.7.7 (metric 20) from 10.5.5.5 (10.5.5.5)
      Origin IGP, metric 0, localpref 50, valid, internal, backup/repair
      Extended Community: RT:100:1 RT:200:1 RT:300:1 RT:400:1
      Originator: 10.7.7.7, Cluster list: 10.5.5.5 , recursive-via-host
      mpls labels in/out 25/17
```

```
  64511
    10.8.8.8 from 10.8.8.8 (192.168.13.1)
      Origin IGP, metric 0, localpref 100, valid, external, best
      Extended Community: RT:100:1 RT:200:1 RT:300:1 RT:400:1 , recursive-via-connected
      mpls labels in/out 25/nolabel
```

The following example shows the additional paths and the BGP recursion flags enabled:

```
Router# show ip bgp vpnv4 vrf test1 192.168.13.1

BGP routing table entry for 400:1:192.168.13.0/24, version 25
Paths: (2 available, best #2, table test1)
  Additional-path
  Advertised to update-groups:
     1
  64511, imported path from 300:1:192.168.13.0/24
    10.7.7.7 (metric 20) from 10.5.5.5 (10.5.5.5)
      Origin IGP, metric 0, localpref 50, valid, internal, backup/repair
      Extended Community: RT:100:1 RT:200:1 RT:300:1 RT:400:1
      Originator: 10.7.7.7, Cluster list: 10.5.5.5 , recursive-via-host
      mpls labels in/out 25/17
  64511
    10.8.8.8 from 10.8.8.8 (192.168.13.1)
      Origin IGP, metric 0, localpref 100, valid, external, best
      Extended Community: RT:100:1 RT:200:1 RT:300:1 RT:400:1 , recursive-via-connected
      mpls labels in/out 25/nolabel
```

The table below describes the significant fields shown in the display.

Table 4: show ip bgp vpnv4 vrf network-address Field Descriptions

Field	Description
BGP routing table entry for ... version	Internal version number of the table. This number is incremented whenever the table changes.
Paths	Number of autonomous system paths to the specified network. If multiple paths exist, one of the multipaths is designated the best path.
Advertised to update-groups	IP address of the BGP peers to which the specified route is advertised.
10.7.7.7 (metric 20) from 10.5.5.5 (10.5.5.5)	Indicates the next hop address and the address of the gateway that sent the update.
Origin	Indicates the origin of the entry. It can be one of the following values: • IGP--Entry originated from Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • incomplete--Entry originated from other than an IGP or Exterior Gateway Protocol (EGP) and was advertised with the **redistribute** router configuration command. • EGP--Entry originated from an EGP.
metric	The value of the interautonomous system metric.
localpref	Local preference value as set with the **set local-preference route-map** configuration command. The default value is 50.

Field	Description
valid	Indicates that the route is usable and has a valid set of attributes.
internal/external	The field is *internal* if the path is learned via iBGP. The field is *external* if the path is learned via eBGP.
best	If multiple paths exist, one of the multipaths is designated the best path and this path is advertised to neighbors.
Extended Community	Route Target value associated with the specified route.
Originator	The router ID of the router from which the route originated when route reflector is used.
Cluster list	The router ID of all the route reflectors that the specified route has passed through.

Related Commands

Command	Description
address-family ipv6	Enters address family configuration mode for configuring routing sessions such as BGP that use standard IPv6 address prefixes.
bgp advertise-best-external	Enables BGP to use an external route as the backup path after a link or node failure.
bgp additional-paths install	Enables BGP to use an additional path as the backup path.

bgp redistribute-internal

To configure iBGP redistribution into an interior gateway protocol (IGP), such as IS-IS or OSPF, use the **bgp redistribute-internal** command in address family or router configuration mode. To stop iBGP redistribution into IGPs, use the **no** form of this command.

bgp redistribute-internal
no bgp redistribute-internal

Syntax Description

This command has no arguments or keywords.

Command Default

In releases prior to Cisco IOS Release 15.1(2)S, 15.2(1)T, and Cisco IOS XE 3.3S, in the IPv4 VRF and IPv6 VRF address families, IBGP routes are not redistributed into IGPs

Beginning with Cisco IOS Release 15.1(2)S, 15.2(1)T, and Cisco IOS XE 3.3S, in the IPv4 VRF and IPv6 VRF address families, IBGP routes are redistributed into IGPs.

For all other address families, IBGP routes are not redistributed into IGPs.

Command Modes

Address family configuration (config-router-af)

Router configuration (config-router)

Command History

Release	Modification
12.1	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)S	This command was modified. In the IPv4 VRF and IPv6 VRF address families, **bgp redistribute-internal** is the default.
15.2(1)T	This command was modified. In the IPv4 VRF and IPv6 VRF address families, **bgp redistribute-internal** is the default.
Cisco IOS XE Release 3.3S	This command was modified. In the IPv4 VRF and IPv6 VRF address families, **bgp redistribute-internal** is the default.

Usage Guidelines

The **bgp redistribute-internal** command is used to configure iBGP redistribution into an IGP. The **clear ip bgp** command must be entered to reset BGP connections after this command is configured.

When redistributing BGP into any IGP, be sure to use IP prefix-list and route-map statements to limit the number of prefixes that are redistributed.

Caution Caution should be exercised when redistributing iBGP into an IGP. Use IP prefix-list and route-map statements to limit the number of prefixes that are redistributed. Redistributing an unfiltered BGP routing table into an IGP can have a detrimental effect on normal IGP network operation.

Examples

In the following example, BGP to OSPF route redistribution is enabled:

```
Router(config)# router ospf 300
Router(config-router)# redistribute bgp 200
Router(config-router)# exit

Router(config)# router bgp 200
Router(config-router)# address-family ipv4
Router(config-router-af)# bgp redistribute-internal
Router(config-router-af)# end
Router# clear ip bgp
 *
```

Related Commands

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

bgp refresh max-eor-time

To cause the router to generate a Route-Refresh End-of-RIB (EOR) message if it was not able to generate one due to route flapping, use the **bgp refresh max-eor-time** command in router configuration mode. To disable the timer, use the **no** form of this command.

bgp refresh max-eor-time *seconds*
no bgp refresh max-eor-time

Syntax Description

seconds	Number of seconds after which, if the router was unable to generate a Route-Refresh EOR message due to route flapping, the router generates a Route-Refresh EOR message. • Valid values are from 600 to 3600, or 0. • The default is 0, meaning the command is disabled.

Command Default

0 seconds

Command Modes

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.

Usage Guidelines

The BGP Enhanced Route Refresh feature is enabled by default. The **bgp refresh max-eor-time** command is not needed under normal circumstances. You might configure the **bgp refresh max-eor-time** command in the event of continuous route flapping, when the router is unable to generate a Route-Refresh EOR message, in which case a Route-Refresh EOR is generated after the timer expires.

Examples

In the following example, if no Route-Refresh EOR message is received after 800 seconds, stale routes will be removed from the BGP table. If no Route-Refresh EOR message is generated after 800 seconds, one is generated.

```
router bgp 65000
 bgp refresh stalepath-time 800
 bgp refresh max-eor-time 800
```

Related Commands

Command	Description
bgp refresh stalepath-time	Causes the router to remove stale routes from the BGP table even if the router does not receive a Route-Refresh EOR message.

bgp refresh stalepath-time

To cause the router to remove stale routes from the BGP table even if the router does not receive a Route-Refresh EOR message, use the **bgp refresh stalepath-time** command in router configuration mode. To disable the timer, use the **no** form of this command.

bgp refresh stalepath-time *seconds*
no bgp refresh stalepath-time

Syntax Description

seconds	Number of seconds the router waits to receive a Route-Refresh End-of-RIB (EOR) message, and then removes the stale paths from BGP table if the router hasn't received an EOR message. • Valid values are 600 to 3600, or 0. • The default is 0, meaning the command is disabled.

Command Default

0 seconds

Command Modes

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.

Usage Guidelines

The BGP Enhanced Route Refresh feature is enabled by default. The **bgp refresh stalepath-time** command is not needed under normal circumstances. You might configure the **bgp refresh stalepath-time** command in the event of continuous route flapping, when the router does not receive a Route-Refresh EOR after an Adj-RIB-Out, in which case the router removes the stale routes from the BGP table after the timer expires. The stale path timer is started when the router receives a Route-Refresh SOR.

Examples

In the following example, if no Route-Refresh EOR message is received after 800 seconds, stale routes will be removed from the BGP table. If no Route-Refresh EOR message is generated after 800 seconds, one is generated.

```
router bgp 65000
 bgp refresh stalepath-time 800
 bgp refresh max-eor-time 800
```

Related Commands

Command	Description
bgp refresh max-eor-time	Causes the router to generate a Route-Refresh EOR message if it was not able to generate one due to route churn.

bgp regexp deterministic

To configure system to use the regular expression engine that internally uses the DFA-based algorithm, use the **bgp regexp deterministic** command in router configuration mode. To configure Cisco IOS software to use the regular expression engine that internally uses the NFA-based algorithm, use the **no** form of this command.

bgp regexp deterministic
no bgp regexp deterministic

Syntax Description

This command has no arguments or keywords.

Command Default

The regular expression engine that internally uses the DFA-based algorithm is enabled.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(22)S	This command was integrated into Cisco IOS Release 12.2(22)S.
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.
15.0(1)M and 12.2(33)XNE	This command was modified. The default changed from the regular expression engine that internally uses the Nondeterministic Finite Automaton-based (NFA-based) algorithm to the regular expression engine that internally uses the Deterministic Finite Automaton-based (DFA-based) algorithm.

Usage Guidelines

This command controls a choice between the use of two different algorithms to evaluate regular expressions.

- The regular expression engine that internally uses the NFA-based algorithm uses a recursive algorithm. This engine is effective, but uses more system resources as the complexity of regular expressions increases. The recursive algorithm works well for simple regular expressions, but is less efficient when processing very complex regular expressions because of the backtracking that is required to process partial matches. In some cases, CPU watchdog timeouts and stack overflow traces have occurred because of the length of time that this engine requires to process very complex regular expressions.
- The regular expression engine that internally uses the DFA-based algorithm is the default engine used. This engine employs an improved algorithm that eliminates excessive backtracking and greatly improves performance when processing complex regular expressions. When this engine is enabled, complex regular expressions are evaluated more quickly, and CPU watchdog timeouts and stack overflow traces will not occur. However, this engine takes longer to process simple regular expressions than the regular expression engine that internally uses the NFA-based algorithm.

Recommendations

- We recommend that you use the regular expression engine that internally uses the DFA-based algorithm if you need to evaluate complex regular expressions or if you have observed problems related to evaluating regular expressions. This engine is enabled by default or re-enabled by entering the **bgp regexp deterministic** command under a Border Gateway Protocol (BGP) routing process.
- We recommend that you use the regular expression engine that internally uses the NFA-based algorithm if you use only simple regular expressions. This engine can be enabled by entering the **no bgp regexp deterministic** command.

Note Only the negative version of the command (**no bgp regexp deterministic)**will appear in a configuration file (nvgened), if configured.

Examples

The following example shows how to configure the software to use the regular expression engine that internally uses the DFA-based algorithm, which is also the default behavior:

```
Router(config)# router bgp 50000
Router(config-router)# bgp regexp deterministic
```

The following examples shows how to configure the software to use the regular expression engine that internally uses the NFA-based algorithm:

```
Router(config)# router bgp 50000
Router(config-router)# no bgp regexp deterministic
```

Related Commands

Command	Description
router bgp	Configures the BGP routing process.
show ip bgp regexp	Displays routes matching the autonomous system path regular expression.

bgp route-map priority

To configure the route map priority for a local Border Gateway Protocol (BGP) routing process, use the **bgp route-map priority** command in address family configuration mode. To remove the route map priority for a local BGP routing process, use the **no** form of this command.

bgp route-map priority
no bgp route-map priority

Command Default

Route map priority is not configured for a local BGP process.

Command Modes

Address family configuration (config-router-af)

Command History

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

Usage Guidelines

The **bgp route-map priority** command is used to configure the route map priority for the local Border Gateway Protocol (BGP) routing process. The specified route map will take priority over the bgp next-hop unchanged and bgp next-hop unchanged allpaths settings.

Examples

The following example shows how to configure the local router with route map priority:

```
router bgp 50000
address-family ipv4 unicast vrf inside
 bgp route-map priority
```

Related Commands

Command	Description
set ip next-hop self	Configures local routes with next hop of self (for BGP only).

bgp router-id

To configure a fixed router ID for the local Border Gateway Protocol (BGP) routing process, use the **bgp router-id** command in router or address family configuration mode. To remove the fixed router ID from the running configuration file and restore the default router ID selection, use the **no** form of this command.

Router Configuration
bgp router-id {*ip-address* | **vrf auto-assign**}
no bgp router-id [**vrf auto-assign**]

Address Family Configuration
bgp router-id {*ip-address* | **auto-assign**}
no bgp router-id

Syntax Description

ip-address	Router identifier in the form of an IP address.
vrf	Configures a router identifier for a Virtual Routing and Forwarding (VRF) instance.
auto-assign	Automatically assigns a router identifier for each VRF.

Command Default

The following behavior determines local router ID selection when this command is not enabled:

- If a loopback interface is configured, the router ID is set to the IP address of the loopback interface. If multiple loopback interfaces are configured, the router ID is set to the IP address of the loopback interface with the highest IP address.
- If no loopback interface is configured, the router ID is set to the highest IP address on a physical interface.

Command Modes

Address family configuration (config-router-af)

Router configuration (config-router)

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	The **vrf**and **auto-assign** keywords were added, and this command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command, including the **vrf**and **auto-assign** keywords, was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command, including the **vrf**and **auto-assign** keywords, was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	The **vrf**and **auto-assign** keywords were added.

Usage Guidelines

The **bgp router-id** command is used to configure a fixed router ID for the local BGP routing process. The router ID is entered in IP address format. Any valid IP address can be used, even an address that is not locally configured on the router. If you use an IP address from a local interface, we recommend that you use the

address of a loopback interface rather than the address of a physical interface. (A loopback interface is more effective than a fixed interface as an identifier because there is no physical link to go down.) Peering sessions are automatically reset when the router ID is changed.

In Cisco IOS Release 12.2(33)SRA, 12.2(31)SB2, 12.2(33)SXH, 12.4(20)T, and later releases, the Per-VRF Assignment of BGP Router ID feature introduced VRF-to-VRF peering in BGP on the same router. BGP is designed to refuse a session with itself because of the router ID check. The per-VRF assignment feature allows a separate router ID per VRF. The router ID can be manually configured for each VRF or automatically assigned either for each VRF or globally under address family configuration mode.

Examples

The following example shows how to configure the local router with a fixed BGP router ID of 192.168.254.254:

```
router bgp 50000
 bgp router-id 192.168.254.254
```

The following example shows how to configure a BGP router ID for the VRF named VRF1. This configuration is done under address family IPv4 VRF configuration mode.

```
router bgp 45000
 address-family ipv4 vrf VRF1
  bgp router-id 10.1.1.99
```

The following example shows how to configure an automatically assigned VRF BGP router ID for all VRFs. This configuration is done under BGP router configuration mode.

```
router bgp 45000
 bgp router-id vrf auto-assign
```

The following example shows how to configure an automatically assigned VRF BGP router ID for a single VRF. This configuration is done under address family IPv4 VRF configuration mode.

```
router bgp 45000
 address-family ipv4 vrf VRF2
  bgp router-id auto-assign
```

Related Commands

Command	Description
show ip bgp	Displays entries in the BGP routing table.
show ip bgp vpnv4	Displays VPNv4 address information from the BGP routing table.

bgp rpki server

To connect to a Resource Public Key Infrastructure (RPKI) server and enable the validation of Border Gateway Protocol (BGP) prefixes based on the autonomous system (AS) from which the prefix originates, use the **bgp rpki server** command in router configuration mode. To stop the connection to the RPKI server and stop the validation of BGP prefixes based on the origin AS, use the **no** form of this command.

bgp rpki server tcp {*ipv4-address ipv6-address*} **port** *port-number* **refresh** *seconds*
no bgp rpki server tcp{*ipv4-address ipv6-address*}**port** *port-number* **refresh** *seconds*

Syntax Description

tcp	Specifies the protocol used by the router to communicate with the RPKI server.
ipv4-address	IPv4 address of the RPKI server.
ipv6-address	IPv6 address of the RPKI server.
port *port-number*	Specifies the 16-bit port number of the RPKI server, in the range from 1 to 65535.
refresh *seconds*	Specifies the refresh interval (in seconds) at which the system will download SOVC records from the RPKI server. • The range is from 1 to 65535.

Command Default

The router is not connected to an RPKI server.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
XE 3.5S	This command was introduced.
15.2(1)S	This command was integrated into Cisco IOS Release 15.2(1)S.
15.2(4)S	This command was implemented on the Cisco 7200 series routers.

Usage Guidelines

Use this command to enable the BGP—Origin AS Validation feature. A separate, external RPKI server must be configured, and its address and port number known. The actual authentication of public key certificates is done on the RPKI server.

If more than one RPKI server is configured, the router will connect to all configured servers and download prefix information from all of them.

After configuration or upon bootup, the router will open a TCP connection to the RPKI server at the specified address and port number. If the connection attempt fails, the router will retry the connection once per minute.

Examples

The following example configures BGP to connect to the RPKI server at 192.168.1.1 and download a list of prefixes and permitted origin AS numbers. Once every 600 seconds the router will query the server to obtain any new prefixes that the server might send.

```
Router(config)# router bgp 65000
Router(config-router)# bgp rpki server tcp 192.168.1.1 port 1033 refresh 600
```

Related Commands

Command	Description
bgp bestpath prefix-validate	Determines whether invalid prefixed are allowed to be used as the best path, even if valid prefixes are available, or disables the checking of prefixes.
clear ip bgp rpki server	Purges SOVC records downloaded from the specified server, and optionally closes the TCP connection to the indicated cache server.
debug ip bgp event rpki	Provides details about RPKI events.
neighbor announce rpki state	Sends and receives the RPKI state and prefix/AS pairs to and from an IBGP neighbor.
show ip bgp ipv4	Displays entries in the BGP IPv4 routing table.
show ip bgp ipv6 unicast	Displays entries in the BGP IPv6 unicast routing table.
show ip bgp rpki servers	Displays the current state of communication with the RPKI servers.
show ip bgp rpki table	Displays the current cached list of prefix/AS pairs.
show ip bgp summary	Displays information about how many prefix/AS pairs are in each RPKI state.

bgp rr-group

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

bgp rr-group *extcom-list-number*
no bgp rr-group *extcom-list-number*

Syntax Description

extcom-list-number	Extended community-list that defines the route targets that will be permitted by the route-reflector group. The range of t numbers that can be entered is from 1 to 500. Only one extended community-list is specified for each route-reflector group.

Command Default

No default behavior or values

Command Modes

Address family configuration (config-router-af)

Command History

Release	Modification
12.1	This command was introduced.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.0(22)S	The maximum number of extended community-lists that can supported by a route-reflector group was changed from 199 to 500 in Cisco IOS Release 12.0(22)S.
12.2(15)T	The maximum number of extended community-lists that can supported by a route-reflector group was changed from 199 to 500 in Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **bgp rr-group**command is used to partition large VPNv4 Border Gateway Protocol (BGP) networks into smaller route-reflector groups. Each route-reflector group permits only routes from route targets defined in an extended community list. Only one extended community list can be configured for each route-reflector group.

Examples

In the following example, a route-reflector group is created. The route target is associated with the VRF and then defined in an extended community list. This route reflector will accept routes from only route target 50000:1024.

```
Router(config)# ip vrf RED
Router(config-vrf)# rd 50000:10000
Router(config-vrf)# route-target both 50000:10000
Router(config-vrf)# route-target export 50000:1024
Router(config-vrf)# exit
```

```
Router(config)# ip extcommunity-list 1 permit rt 50000:1024
Router(config)# router bgp 50000
Router(config-router)# address family vpnv4

Router(config-router-af)# bgp rr-group 1
Router(config-router-af)# neighbor 192.168.0.1 activate

Router(config-router-af)# neighbor 192.168.0.1 route-reflector-client
Router(config-router-af)# neighbor 192.168.0.1 send-community extended
Router(config-router-af)# end
```

Related Commands

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

bgp scan-time

To configure scanning intervals of Border Gateway Protocol (BGP) routers for next hop validation or to decrease import processing time of Virtual Private Network version 4 (VPNv4) routing information, use the **bgp scan-time** command in address family or router configuration mode. To return the scanning interval of a router to its default scanning interval of 60 seconds, use the **no** form of this command.

bgp scan-time [**import**] *scanner-interval*
no bgp scan-time [**import**] *scanner-interval*

Syntax Description

import	(Optional) Configures import processing of VPNv4 unicast routing information from BGP routers into routing tables.
scanner-interval	The scanning interval in seconds of BGP routing information. Valid values are from 5 to 60. The default is 60.

Command Default

The default scanning interval is 60 seconds.

Command Modes

Address family configuration (config-router-af)

Router configuration (config-router)

Command History

Release	Modification
12.0(7)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.
15.0(1)M	This command was modified. The **import** keyword was removed. It is not available in Cisco IOS Release 15.0(1)M and later Cisco IOS Release 15.0M releases.
12.2(33)SRE	This command was modified. The **import** keyword was removed. It is not available in Cisco IOS Release 12.2(33)SRE and later Cisco IOS Release 12.2SR releases.
Cisco IOS XE 2.6	This command was integrated into Cisco IOS XE Release 2.6.
15.1(2)T	This command was modified. The minimum scan time was increased from 5 seconds to 15 seconds.
15.0(1)S	This command was modified. The minimum scan time was increased from 5 seconds to 15 seconds.
Cisco IOS XE 3.1S	This command was modified. The minimum scan time was increased from 5 seconds to 15 seconds.
15.0(1)SY	This command was integrated into Cisco IOS Release 15.0(1)SY.

Release	Modification
Cisco IOS XE 3.4.1S	This command was modified. The minimum scan time was decreased from 15 seconds to 5 seconds. The command can be configured even if NHT is enabled.
15.1(3)S1	This command was modified. The minimum scan time was decreased from 15 seconds to 5 seconds. The command can be configured even if NHT is enabled.

Usage Guidelines

Entering the **no** form of this command does not disable scanning, but removes it from the output of the **show running-config** command.

The **import** keyword is supported in address family VPNv4 unicast mode only.

The BGP Event Based VPN Import feature introduced a modification to the existing BGP path import process using new commands and the **import** keyword was removed from the **bgp scan-time** command in Cisco IOS Release 15.0(1)M, 12.2(33)SRE, and later releases.

While **bgp nexthop** address tracking (NHT) is enabled for an address family, the **bgp scan-time** command will not be accepted in that address family and will remain at the default value of 60 seconds. NHT must be disabled before the **bgp scan-time** command will be accepted in either router mode or address family mode. However, for Cisco IOS Release 15.1(3)S1 and Cisco IOS XE Release 3.4.1S, the **bgp scan-time** command can be configured even if NHT is enabled.

Examples

In the following router configuration example, the scanning interval for next hop validation of IPv4 unicast routes for BGP routing tables is set to 20 seconds:

```
router bgp 100
 no synchronization
 bgp scan-time 20
```

In the following address family configuration example, the scanning interval for next hop validation of address family VPNv4 unicast routes for BGP routing tables is set to 45 seconds:

```
router bgp 150
 address-family vpnv4 unicast
  bgp scan-time 45
```

In the following address family configuration example, the scanning interval for importing address family VPNv4 routes into IP routing tables is set to 30 seconds:

```
router bgp 150
 address-family vpnv4 unicast
  bgp scan-time import 30
```

Related Commands

Command	Description
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
bgp nexthop	Configures BGP next-hop address tracking.

bgp slow-peer detection

To specify a threshold time that dynamically determines a slow peer, use the **bgp slow-peer detection** command in address-family configuration mode. To restore the default value, use the **no** form of this command.

bgp slow-peer detection [**threshold** *seconds*]
no bgp slow-peer detection

Syntax Description

seconds	(Optional) Threshold time in seconds that the timestamp of the oldest message in a peers queue can be lagging behind the current time before the peer is determined to be a slow peer. The range is from 120 to 3600; the default is 300.

Command Default

300 seconds

Command Modes

Address-family configuration (config-router-af)

Command History

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

Usage Guidelines

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

Note If you want detection for only some peers, use the **neighbor slow-peer detection** command. The **neighbor slow-peer detection** command overrides the **bgp slow-peer detection**command. If the **neighbor slow-peer detection** command is unconfigured or if **no neighbor slow-peer detection** is configured, the system will inherit the global, address-family level configuration.

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

Examples

The following example specifies that if the timestamp on a peer's update message is more than 360 seconds before the current time, the peer that sent the update message is marked as a slow peer.

```
Router(config-router-af)# bgp slow-peer detection threshold 360
```

Related Commands

Command	Description
bgp slow-peer split-update-group dynamic	Moves a dynamically detected slow peer to a slow update group.
clear ip bgp slow	Moves dynamically configured slow peers back to their original update groups.

bgp slow-peer split-update-group dynamic

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

bgp slow-peer split-update-group dynamic [**permanent**]
no bgp slow-peer split-update-group dynamic

Syntax Description

permanent	(Optional) Specifies that after the slow peer becomes a regular peer (converges), it is not moved back to its original update group automatically. After resolving the root cause of the slow peer, (network congestion, and so forth), the network administrator can use one of the **clear** commands to move the peer to its original update group.

Command Default

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

Command Modes

Address-family configuration (config-router-af)

Command History

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

Usage Guidelines

When a peer is dynamically detected to be a slow peer (based on the threshold of the **bgp slow-peer detection** command), the slow peer is moved to a slow update group. If a *static* slow peer update group exists, (based on the **neighbor slow-peer split-update-group static** command, the dynamic slow peer is moved to the static slow peer update group; otherwise, a new slow peer update group is created and the peer is moved to that group. Furthermore:

- If the **permanent** keyword is configured, the peer is not automatically moved to its original update group. This is the recommended option. You can the **clear ip bgp slow**command to move the peer back to its original update group.
- If the **permanent** keyword is not configured, the slow peer will be moved back to its regular original update group after it becomes a regular peer (converges).

Note The **neighbor slow-peer split-update-group dynamic**command performs the same function as the **bgp slow-peer split-update-group dynamic** command (at the address-family level), except that the **neighbor slow-peer split-update-group dynamic** command overrides the address-family level command. When the **neighbor slow-peer split-update-group dynamic** command is unconfigured, the system will function according to the address-family level configuration. The **slow-peer split-update-group dynamic** command performs the same function through a peer policy template.

If **bgp slow-peer split-update-group dynamic**is configured, but no slow peer detection is configured, the detection will be done at the default threshold of 300 seconds.

Examples

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

```
Router(config-router-af)# bgp slow-peer detection threshold 360
Router(config-router-af)# bgp slow-peer split-update-group dynamic
```

Related Commands

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

bgp soft-reconfig-backup

To configure a Border Gateway Protocol (BGP) speaker to perform inbound soft reconfiguration for peers that do not support the route refresh capability, use the **bgp soft-reconfig-backup** command in address-family or r outer configuration mode. To disable this function, use the **no** form of this command.

bgp soft-reconfig-backup
no bgp soft-reconfig-backup

Syntax Description

This command has no arguments or keywords.

Command Default

Inbound soft reconfiguration for peers that do not support the route refresh capability is not performed.

Command Modes

Address-family configuration (config-router-af)

Router configuration (config-router)

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

The **bgp soft-reconfig-backup** command is used to configure BGP to perform inbound soft reconfiguration for peers that do not support the route refresh capability. The configuration of this command allows you to configure BGP to store updates (soft reconfiguration) only as necessary. Peers that support the route refresh capability are unaffected by the configuration of this command.

Use the **show ip bgp neighbors** command to determine if a peer supports the route refresh capability. If supported, the following will be displayed in the output:

```
Route refresh: advertised and received(new)
```

Use the **show ip bgp** command to determine if the BGP speaker is storing inbound updates for peer that does not support the route refresh capability. If updates are stored, the following will be displayed in the output:

```
(received-only)
```

Examples

The following example, starting in Global configuration mode, configures the router perform inbound soft reconfiguration only if the peer does not support the route refresh capability:

```
Router(config)# router bgp 50000
Router(config-router)# bgp soft-reconfig-backup

Router(config-router)# neighbor 10.1.1.1 remote-as 40000

Router(config-router)# neighbor 192.168.1.1 remote-as 60000
```

Related Commands

Command	Description
show ip bgp	Displays entries in the Border Gateway Protocol (BGP) routing table.

Command	Description
show ip bgp neighbors	Displays information about the TCP and Border Gateway Protocol (BGP) connections to neighbors.

bgp sourced-paths

To enable the sourcing of multiple paths redistributed per protocol into the into the Border Gateway Protocol (BGP) from the Routing Information Base (RIB), use the **bgp sourced-paths** command. To disable the configuration or return to the default, use the **no** form of this command.

bgp sourced-paths per-net {**isis** | **ospf** | **ospfv3** | **static**} **all**
no bgp sourced-paths per-net {**isis** | **ospf** | **ospfv3** | **static**} **all**

Syntax Description

per-net	Allows per-network sourcing of multiple paths.
isis	Allows sourcing of multiple paths from the Intermediate System-to-Intermediate System (IS-IS) protocol.
ospf	Allows sourcing of multiple paths from the Open Shortest Path First (OSPF) protocol.
ospfv3	Allows sourcing of multiple paths from the OSPF Version 3 (OSPFv3) protocol.
static	Allows sourcing of multiple static paths.
all	Allows sourcing of all sourced paths or next hops in the RIB.

Command Default

Only one path is redistributed into BGP from the RIB.

Command Modes

Address family configuration (config-router-af)

Command History

Release	Modification
Cisco IOS XE Release 3.15S	This command was introduced.

Usage Guidelines

The **bgp sourced-paths** command is supported for both **address-family ipv4** and **address-family ipv6** commands.

The paths that are sourced with 0.0.0.0 as the gateway will not have multiple paths redistributed into BGP.

Examples

The following example shows how to redistribute multiple paths into BGP.

```
Device# configure terminal
Device(config)# router bgp 65000
Device(config-router)# address-family ipv4 vrf blue
Device(config-router-af)# bgp sourced-paths per-net isis all
Device(config-router-af)# redistribute isis 1
Device(config-router-af)# end
```

```
Device# configure terminal
Device(config)# router bgp 65000
Device(config-router)# address-family ipv6 multicast
Device(config-router-af)# bgp sourced-paths per-net static all
Device(config-router-af)# redistribute static
Device(config-router-af)# end
```

Related Commands

Command	Description
address-family ipv4	Enters address family or router scope address family configuration mode to configure a routing session using standard IPv4 address prefixes.
address-family ipv6	Enters address family configuration mode for configuring routing sessions, such as BGP, that use standard IPv6 address prefixes.
redistribute isis	Redistributes routes from one routing domain into another routing domain using IS-IS as both the target and source protocol.
redistribute static	Redistributes static routes.
router bgp	Configures the BGP routing process.

bgp sso route-refresh-enable

To enable BGP to send route-refresh requests to nonstop routing (NSR) peers in the event of an RP failover, use the **bgp sso route-refresh-enable** command in router configuration mode. To disable the sending of route-refresh requests to NSR peers in the event of an RP failover, use the **no** form of this command.

bgp sso route-refresh-enable
no bgp sso route-refresh-enable

Syntax Description

This command has no arguments or keywords.

Command Default

Route-refresh requests are not sent to NSR peers in the event of a failover.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
15.2(2)S	This command was introduced.
Cisco IOS XE Release 3.6S	This command was integrated into Cisco IOS XE Release 3.6S.

Usage Guidelines

By default, if an Active RP fails, the new Active RP does not send route-refresh requests to NSR peers because it creates unnecessary churn during switchover from the Standby RP to the Active RP. Use the **bgp sso route-refresh-enable** command only if, for some reason, you want the new Active RP to send route-refresh requests to NSR peers upon failover.

Examples

The following example shows how to configure BGP to send route-refresh requests to NSR peers in the event of a failover:

```
Router(config-router)# bgp sso route-refresh-enable
```

Related Commands

Command	Description
show ip bgp vpnv4 all neighbor	Displays information about BGP peers.
show ip bgp vpnv4 all sso summary	Displays the number of BGP peers that support BGP NSR with stateful switchover.

bgp suppress-inactive

To suppress the advertisement of routes that are not installed in the routing information base (RIB), use the **bgp suppress-inactive** command in address family or router configuration mode.

bgp suppress-inactive
no bgp suppress inactive

Syntax Description

This command has no arguments or keywords.

Command Default

No routes are suppressed.

Command Modes

Address family configuration (config-router-af)

Router configuration (config-router)

Command History

Release	Modification
12.2(11)T	This command was introduced.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
15.1S	This command was modified. Support for IPv6 and VRFv6 address families was added.

Usage Guidelines

The **bgp suppress-inactive** command is used to prevent routes that are not installed in the RIB (inactive routes) from being advertised to peers. If this feature is not enabled or if the **no** form of this command is used, Border Gateway Protocol (BGP) will advertise inactive routes.

Note BGP marks routes that are not installed into the RIB with a RIB-failure flag. This flag will also appear in the output of the **show ip bgp** command; for example, Rib-Failure (17). This flag does not indicate an error or problem with the route or the RIB, and the route may still be advertised depending on the configuration of this command. Enter the **show ip bgp rib-failure** command to see more information about the inactive route.

In certain scenarios, routes that were not installed in the RIB due to a temporary failure are installed at a later point in time, depending on the reason for the failure. After successful installation, the advertisement of the routes continue.

Examples

In the following example, the BGP routing process is configured for IPv4 address family to not advertise routes that are not installed in the RIB:

```
Device(config)# router bgp 500000
Device(config-router)# address-family ipv4
Device(config-router)# bgp suppress-inactive
```

In the following example, the BGP routing process is configured for IPv6 address family to not advertise routes that are not installed in the RIB:

```
Device(config)# router bgp 500000
Device(config-router)# address-family ipv6
Device(config-router)# bgp suppress-inactive
```

Related Commands

Command	Description
clear ip bgp	Resets a BGP connection using BGP soft reconfiguration.
show ip bgp rib-failure	Display BGP routes were not installed in the RIB.

bgp transport

To enable TCP transport session parameters globally for all Border Gateway Protocol (BGP) sessions, use the **bgp transport** command in router configuration mode. To disable TCP transport session parameters globally for all BGP sessions, use the **no** form of this command.

bgp transport path-mtu-discovery
no bgp transport path-mtu-discovery

Syntax Description

path-mtu-discovery	Enables transport path maximum transmission unit (MTU) discovery.

Command Default

TCP path MTU discovery is enabled by default for all BGP sessions.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
12.2(33)SRA	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

This command is enabled by default because it is used to allow BGP sessions to take advantage of larger MTU links, which can be very important for internal BGP (iBGP) sessions. Use the **show ip bgp neighbors** command to ensure that TCP path MTU discovery is enabled.

Examples

The following example shows how to disable TCP path MTU discovery for all BGP sessions:

```
router bgp 45000
 no bgp transport path-mtu-discovery
```

The following example shows how to enable TCP path MTU discovery for all BGP sessions:

```
router bgp 45000
 bgp transport path-mtu-discovery
```

Related Commands

Command	Description
neighbor transport	Enables transport session parameters for a BGP neighbor session.
show ip bgp neighbors	Displays information about BGP and TCP connections to neighbors.

bgp update-delay

To set the maximum initial delay period before a Border Gateway Protocol (BGP)-speaking networking device sends its first updates, use the **bgp update-delay** command in router configuration mode. To remove the **bgp update-delay** command from the configuration file and restore the initial delay to its default value, use the **no** form of this command.

bgp update-delay *seconds*
no bgp update-delay

Syntax Description

seconds	The maximum delay, in seconds, before a BGP-speaking networking device sends its updates. The range is from 0 to 3600. The default is 120 seconds.

Command Default

If this command is not configured, the default initial delay value is 120 seconds.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
12.2	This command was introduced.
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

When BGP is started, it waits a specified period of time for its neighbors to be established themselves and to begin sending their initial updates. Once that period is complete, or when the time expires, the best path is calculated for each route, and the software starts sending advertisements out to its peers. This behavior improves convergence time because, if the software were to start sending advertisements out immediately, it would have to send extra advertisements if it later received a better path for the prefix from another peer.

The **bgp update-delay** command is used to tune the maximum time the software will wait after the first neighbor is established until it starts calculating best paths and sending out advertisements. This command can be used when configuring the **bgp graceful-restart** command as part of the Nonstop Forwarding (NSF) capability.

Examples

The following example sets the maximum initial delay to 240 seconds:

```
router bgp 65000
 bgp update-delay 240
```

Related Commands

Command	Description
bgp graceful-restart	Enables the BGP graceful restart capability.

bgp update-group split as-override

To keep peers that are configured with **neighbor as-override** in separate, single-member update groups, use the **bgp update-group split as-override** command in address-family configuration mode. To restore the peers back to the original state of uniting with other peers under the same VRF configured with the same policies, use the **no** form of this command.

bgp update-group split as-override
no bgp update-group split as-override

Syntax Description

This command has no arguments or keywords.

Command Default

BGP update groups are not split based on a policy of AS-override.

Command Modes

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

Command History

Release	Modification
12.2(33)SRD4	This command was introduced.
15.1(4)S	Support for VPNv6 and VPNv4 multicast address family configuration modes were added.

Usage Guidelines

When the **neighbor as-override** command is specified to configure that a PE router overrides the autonomous system number (ASN) of a site with the ASN of a provider, it is standard practice to also configure Site of Origin (SoO). SoO prevents the route originated by a CE towards a PE from being sent back to the same CE by the PE.

An alternative to the SoO feature is using the **bgp update-group split as-override** command. The **bgp update-group split as-override** command causes the peers configured with the **neighbor as-override** command under the same IPv4 VRF, which were previously under one update group, to be removed (split) from that update group and each placed in their own update group (each becoming the only member in an update group).

This command is supported in the following address families:

- VPNv4 unicast
- VPNv4 multicast
- VPNv6 unicast
- VPNv6 multicast
- MVPNv4
- MVPNv6

Note The **bgp update-group split as-override** command cancels the resource optimization during update generation that was achieved by having the peers under the same VRF with common outbound policies belong to the same update group.

Examples

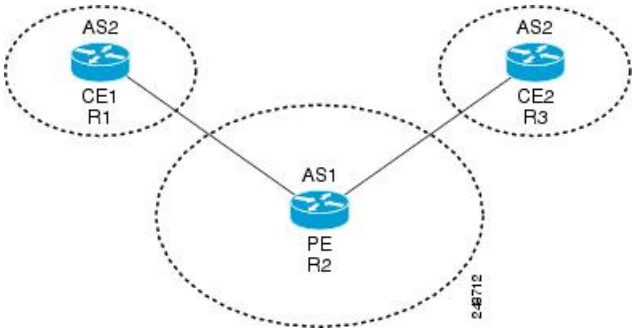
In the following example, the **neighbor as-override** command is configured on a PE for neighbors CE1 and CE2. When CE1 advertises a route to the PE, this command replaces the peer AS number (2) in the AS path with its own AS number (1) before advertising the route to its peers, in this case, CE2. Enabling the AS override feature allows routes originating from an AS to be accepted by another router (CE2) residing in the same AS. Without AS override enabled, CE2 would refuse the route advertisement once the AS path shows that the route originated from its own AS (2). This behavior occurs by default to prevent route loops. The **neighbor as-override** command overrides this default behavior.

If these PE peers, CE1 and CE2, under the **address-family ipv4 vrf** *name* command have the **neighbor as-override** configured on the PE, by default they are placed in the same update group. This causes the source router, CE1, to receive back its own prefix, since it's part of an update group [with CE1 and CE2] to which the prefix is advertised. This situation might result in route loops if not properly configured or if **neighbor as-override** is not accompanied by a feature such as SoO.

An alternative to SoO is to use the **bgp update-group split as-override** command. This command configured under **address-family vpnv4**, causes peers with **neighbor as-override** configured under **address-family ipv4 vrf** *name* to be put in separate update groups. As a result of this update-group segregation, the prefixes sent out by a router, say CE1, do not get returned to itself by the PE.

The **bgp update-group split as-override** command, although configured under address family VPNv4, splits only the peers configured under address family IPv4 VRF B and no peers configured under any other address family. The figure below illustrates the PE in AS1 and the two CEs in AS2.

Figure 5: Example of bgp update-group split as-override Scenario



The configuration for the PE (Router 2) follows:

```
Router2(config)# router bgp 1
Router2(config-router)# address-family ipv4 vrf B
Router2(config-router-af)# neighbor 192.168.11.2 as-override
Router2(config-router-af)# neighbor 192.168.14.3 as-override
Router2(config-router-af)# exit
Router2(config-router)# address-family vpnv4
Router2(config-router-af)# bgp update-group split as-override
Router2(config-router-af)# exit-address-family
```

Related Commands

Command	Description
neighbor as-override	Configures a provider edge (PE) router to override the autonomous system number (ASN) of a site with the ASN of a provider.
neighbor soo	Sets the site-of-origin (SoO) value for a BGP neighbor or peer group.

bgp upgrade-cli

To upgrade a Network Layer Reachability Information (NLRI) formatted router configuration file to the address-family identifier (AFI) format and set the router command-line interface (CLI) to use only AFI commands, use the **bgp upgrade-cli** command in router configuration mode.

bgp upgrade-cli

Syntax Description

This command has no keywords or arguments.

Command Default

NLRI commands are not upgraded to the AFI format.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
12.0(14)ST	This command was introduced.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **bgp upgrade-cli** command is used to upgrade a router that is running in the NLRI formatted CLI to the AFI CLI format. The upgrade is automatic and does not require any further configuration by the network operator, and no configuration information is lost but you cannot return to the NLRI configuration because a **no** form does not exist for this command. Several NLRI-based commands do not exist under the AFI format but have equivalent commands under the AFI format. See the table below for NLRI to AFI command mapping.

Table 5: Mapping NLRI Commands with Address Family Commands

NLRI Commands	Address Family Command
distance mbgp	**distance bgp**
match nlri	**address-family ipv4**
set nlri	**address-family ipv4**
show ip mbgp	**show ip bgp ipv4 multicast**
show ip mbgp summary	**show ip bgp ipv4 multicast summary**

Examples

In the following example, the existing NLRI router configuration file is converted to the AFI format and the router is configured to use only AFI format commands:

```
Router(config)#
router bgp 5
Router(config-router)#
bgp upgrade-cli
```

bgp-policy

To enable Border Gateway Protocol (BGP) policy accounting or policy propagation on an interface, use the **bgp-policy** command in interface configuration mode. To disable BGP policy accounting or policy propagation, use the **no** form of this command.

bgp-policy {**accounting** [{**input** | **output**} [**source**]] | **destination** {**ip-prec-map** | **ip-qos-map**} | **source** {**ip-prec-map** | **ip-qos-map**}}
no bgp-policy {**accounting** [{**input** | **output**}] | **destination** {**ip-prec-map** | **ip-qos-map**} | **source** {**ip-prec-map** | **ip-qos-map**}}

Syntax Description

accounting	Enables accounting policy on the basis of community lists, autonomous system numbers, or autonomous system paths.
input	(Optional) Enables accounting policy on the basis of traffic that is traveling through an input interface.
output	(Optional) Enables accounting policy on the basis of traffic that is traveling through an output interface.
source	Enables accounting policy on the basis of the source address. This keyword is optional when used with the **accounting** keyword.
destination	Enables accounting policy on the basis of the destination address.
ip-prec-map	(Optional) Enables quality of service (QoS) policy on the basis of the IP precedence.
ip-qos-map	(Optional) Enables packet classification on the basis of the specified QoS group.

Command Default

BGP policy accounting and policy propagation are not enabled on an interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.1CC	This command was introduced.
12.0(9)S	This command was integrated into Cisco IOS Release 12.0(9)S and the **accounting** keyword was added.
12.0(17)ST	This command was integrated into Cisco IOS Release 12.0(17)ST.
12.0(22)S	The **input**, **output**, and **source** keywords were added for the Cisco 7200 series and Cisco 7500 series platforms.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(4)T	The **input**, **output**, and **source** keywords were integrated into Cisco IOS Release 12.3(4)T.

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

For BGP policy propagation to function, you must enable BGP and either Cisco Express Forwarding (CEF) or distributed CEF (dCEF).

To specify the QoS policy based on the IP precedence or a QoS group, the proper route-map configuration must be in place (for example, the **set ip precedence** or **set qos-group** route-map configuration command). To display QoS policy information for the interface, use the **show ip interface** command.

Note If you specify both the sourceand destination addresses when configuring policy propagation based on an access control list (ACL), the software looks up the source address in the routing table and classifies the packet based on the source address first; then the software looks up the destination address in the routing table and reclassifies the packet based on the destination address.

To specify the accounting policy, the proper route-map configuration must be in place matching specific BGP attributes using the **set traffic-index**command. In BGP router configuration mode, use the **table-map** command to modify the accounting buckets when the IP routing table is updated with routes learned from BGP. To display accounting policy information, use the **show cef interface policy-statistics**, **show ip bgp**, and **show ip cef detail** EXEC commands.

Examples

In the following example, the BGP policy propagation feature is enabled on an interface based on the source address and the IP precedence setting:

```
Router(config)# interface ethernet 4/0/0
Router(config-if)# bgp-policy source ip-prec-map
Router(config-if)# end
```

In the following example, the BGP policy accounting feature is configured using a source address on input traffic being enabled on GE-WAN interface 9/1. The policy is classified by autonomous system paths.

```
Router(config)# router bgp 50000

Router(config-router)# no synchronization
Router(config-router)# table-map buckets

Router(config-router)# exit
Router(config)# ip as-path access-list 1 permit _10_

Router(config)# ip as-path access-list 2 permit _11_

Router(config)# route-map buckets permit 10
Router(config-route-map)# match as-path 1
Router(config-route-map)# set traffic-index 1

Router(config-route-map)# exit
```

```
Router(config)# route-map buckets permit 20

Router(config-route-map)# match as-path 2

Router(config-route-map)# set traffic-index 2

Router(config-route-map)# exit

Router(config)# route-map buckets permit 80
Router(config-route-map)# set traffic-index 7
Router(config-route-map)# exit
Router(config)# interface GE-WAN9/1

Router(config-int)# ip address 10.0.2.2 255.255.255.0

Router(config-int)# bgp-policy accounting input source

Router(config-int)# no negotiation auto

Router(config-int)# end
```

Related Commands

Command	Description
set ip precedence	Sets the precedence values in the IP header.
set qos-group	Sets a QoS group ID to classify packets.
set traffic-index	Defines where to output packets that pass a match clause of a route map for BGP policy accounting.
show cef interface policy-statistics	Displays detailed CEF policy statistical information for all interfaces.
show ip bgp	Displays entries in the BGP routing table.
show ip cef	Displays entries in the FIB or FIB summary information.
show ip interface	Displays the usability status of interfaces.
table-map	Classifies routes according to a route map.

bmp

To configure BGP monitoring protocol (BMP) parameters for BGP neighbors and to enter the BMP server configuration mode to configure BMP servers, use the **bmp** command in router configuration mode. To disable configuration of the BMP neighbors and servers, use the **no** form of the command.

bmp {**buffer-size** *buffer-bytes* | **initial-refresh** {**delay** *refresh-delay* | **skip**} | **server** *server-number-n*}

no bmp {**buffer-size** *buffer-bytes* | **initial-refresh** {**delay** *refresh-delay* | **skip**} | **server** *server-number-n*}

Syntax Description

buffer-size *buffer-bytes*	Sets the BMP buffer size, in MB, for input-output (I/O) operations in a BGP neighbor. The value that you can set for the *buffer-bytes* argument ranges from 1 to 2048 MB.
initial-refresh	Configures the initial refresh options to handle refresh requests sent by BMP servers to BGP BMP neighbors.
delay *refresh-delay*	Sets the delay, in seconds, before initial refresh request is sent by a BMP server to a BGP BMP neighbor. The delay that you can set ranges from 1 to 3600 seconds.
skip	Configures BMP to skip any refresh requests sent by a BMP server to a BGP BMP neighbor.
server *server-number-n*	Configures BMP monitoring on a specific BGP BMP server. The value of n ranges from 1 to 4. You can randomly specify any server number to activate BMP monitoring on it. The **server** keyword also enables BMP server configuration mode.

Command Default

BMP configuration for BGP neighbors is disabled by default.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
15.4(1)S	This command was introduced.
Cisco IOS XE Release 3.11S	This command was integrated into Cisco IOS XE Release 3.11S.

Usage Guidelines

While the **neighbor bmp-activate** command activates BMP for BGP neighbors, the **bmp** command configures parameters to establish connection between BGP BMP neighbors and BMP server. Besides configuring parameters such as maximum buffer size, request refresh delay, and request skip; the **bmp server** command enables BMP server configuration mode, which is a sub-mode of router configuration. In BMP server configuration mode, you can configure the following parameters for a specific BMP server:

- Connection of BGP BMP neighbors to BMP servers.
- IP address of BMP servers.
- Description of the BMP servers.
- Failure retry delay in sending BMP server updates.

- Flapping delay in sending BMP server updates.
- Initial delay in sending BMP server updates.
- Setting IP Differentiated Services Code Point (DSCP) values for BMP servers.
- Statistics reporting period for BMP servers.
- Interface source of routing updates.
- Exit from BMP server configuration mode.

Example

The following example shows how to configure initial refresh delay of 30 seconds for BGP neighbors on which BMP is activated using the **neighbor bmp-activate** command:

```
Device> enable
Device# configure terminal
Device(config)# router bgp 65000
Device(config-router)# bmp initial-refresh delay 30
Device(config-router)# end
```

The following is sample output from the **show ip bgp bmp neighbors** command, which displays the refresh value of 30 seconds configured for the BGP BMP neighbors:

```
Device# show ip bgp bmp server neighbors

Number of BMP neighbors configured: 10
BMP Refresh not in progress, refresh not scheduled
Initial Refresh Delay configured, refresh value 30s
BMP buffer size configured, buffer size 2048 MB, buffer size bytes used 0 MB

Neighbor           PriQ      MsgQ      CfgSvr#             ActSvr#             RM Sent
30.1.1.1           0         0         1  2                1  2                16
2001:DB8::2001     0         0         1  2                1  2                15
40.1.1.1           0         0         1  2                1  2                26
2001:DB8::2002     0         0         1  2                1  2                15
50.1.1.1           0         0         1  2                1  2                16
60.1.1.1           0         0         1  2                1  2                26
2001:DB8::2002     0         0         1                   1                   9
70.1.1.1           0         0         2                   2                   12
Neighbor           PriQ      MsgQ      CfgSvr#             ActSvr#             RM Sent
80.1.1.1           0         0         1                   1                   10
2001:DB8::2002     0         0         1  2                1  2                16
```

Related Commands

Command	Description
neighbor bmp-activate	Activates BMP monitoring for BGP neighbors.
show ip bgp bmp	Displays information about BMP servers and neighbors.